Appendix 3: Technical Architecture for Services: Technology Strategy

Table of Contents

List of Figures

List of Tables

1 Introduction

The American Recovery and Reinvestment Act of 2009 (ARRA), through the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), that sets forth a plan for advancing the appropriate use of health information technology (HIT) to improve quality of care and establish a foundation for health care reform. HITECH establishes several new grant programs that will provide resources to promote nationwide use of HIT. Together, they are intended to facilitate the adoption and use of EHRs by providing technical assistance, the capacity to exchange health information, and the availability of trained professionals to support these activities.

The Office of the National Coordinator for Health Information Technology (ONC) within the Department of Health and Human Services (HHS) serves as the principal federal entity charged with coordinating the overall effort to implement a nationwide HIT infrastructure that allows for the electronic use and exchange of health information. The State Health Information Exchange Cooperative Agreements Program sponsored by ONC is a funding opportunity designed to promote health information exchange (HIE) that will advance mechanisms for information sharing across the health care system. Awards under the program are being made in the form of cooperative agreements to states or qualified state-designated entities (SDEs). The purpose of this program is to continuously improve and expand HIE services over time to reach all health care providers in an effort to improve the quality and efficiency of health care. Cooperative agreement recipients will evolve and advance the necessary governance, policies, technical services, business operations and financing mechanisms for HIE over a four year performance period. ONC envisions that this program will build off of existing efforts to advance regional and state level HIE while moving towards nationwide interoperability.

HITECH and the State HIE Cooperative Agreements Program provides a tremendous opportunity to rapidly accelerate implementation of HIT and advance HIE in California. Careful planning is key to realizing the promises of HITECH. The State, in cooperation with ONC, is developing a set of planning documents to guide development of statewide HIE and use of State resources. Key among them is an Implementation Plan for statewide shared services.

1.1 Scope of the Analysis

The overall goal of the set of documents that outline the Technical Architecture for Services is to define Cal eConnect's technical solution for statewide HIE. They describe the technical architecture, and the detailed plan for implementing the architecture and operating and maintaining the components and services it supports.

This document, Technology Strategy, is the first among the document set, and comprises two primary analyses that:

1) summarize the requirements of the meaningful use criteria, nationwide standards for interoperability, the Nationwide Health Information Network (NHIN) standards and services, and State requirements; and
2) outlines a technology strategy for shared services that addresses these requirements.

This analysis will inform the development of an architecture for shared services, including the standards elements of that architecture might support.

1.2 Methodology

This analysis was based primarily upon a set of documents published by the federal government that form the basis for meaningful use and nationwide standards for interoperability. They include:

1) "Medicare and Medicaid Programs; Electronic Health Record Incentive Program; Proposed Rule", published by the Centers for Medicare and Medicaid Services in the Federal Register 13 January 2010, 45 CFR Par 142, *et al*., which can be downloaded from http://edocket.access.gpo.gov/2010/pdf/E9-31217.pdf.
2) "Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology; Interim Final Rule" published by the Department of Health and Human Services in the Federal Register on 13 January 2010, 45 CFR Part 170, which can be downloaded from http://edocket.access.gpo.gov/2010/pdf/E9-31216.pdf.
3) The 2010 Final Production Specifications for the Nationwide Health Information Network provisionally approved by the NHIN Technical Committee and subject to the validation of the NHIN reference implementation, all available on the NHIN section of the HHS web site at http://healthit.hhs.gov (search for NHIN Exchange).
4) Material on the NHIN Direct wiki at http://nhindirect.org/.

In addition, the California Health and Human Services Agency (CHHS) established the California eHealth Technical Advisory Committee and Technical Working Group as consensus organizations to establish a technical strategy for shared services that might be developed under the State HIE Cooperative Agreement Program. Much of the information from the deliberations of these organizations form the basis for the technology strategy. A discussion of that strategy can be found at:

5) "California Health Information Exchange Strategic and Operational Plans" published by CHHS on 31 March 2010, which can be downloaded from http://www.ehealth.ca.gov/LinkClick.aspx?fileticket=zK7zQxE20no%3d&tabid=72.

2 Exchange Requirements

2.1 Meaningful Use

ARRA authorized the Centers for Medicare and Medicaid Services (CMS) to provide incentives through Medicare and Medicaid reimbursements for eligible providers[1] and hospitals successfully becoming "meaningful users of certified electronic health record (EHR) technology". The Medicare and Medicaid programs will provide incentive payments to eligible providers, hospitals, and (in the case of Medicare) critical access hospitals for efforts to adopt, implement, or upgrade certified EHR technology in order to achieve meaningful use in the first

[1] The Office of the National Coordinator for Health Information Technology normally uses "professional" rather than "provider" when referring to meaningful use. Provider is used in this document, as it the more common term in the industry today.

year of their participation in the program and for demonstrating meaningful use during each of five subsequent years.

On 30 December 2009, CMS announced a notice of proposed rulemaking (NPRM) to implement the meaningful use provisions of ARRA, and published the draft rule on 13 January 2010. The proposed rule outlines provisions governing the EHR incentive programs, including defining the central concept of meaningful use of EHR technology. CMS' goal is for the definition of meaningful use to be consistent with applicable provisions of Medicare and Medicaid law while continually advancing the contributions certified EHR technology can make to improving health care quality, efficiency, and patient safety. To accomplish this, CMS' proposed rule would phase in more robust criteria for demonstrating meaningful use in three stages.

The State HIE Cooperative Agreement Program calls for activities in developing health information interoperability in a way that are consistent with and support providers in qualifying for the Medicaid and Medicare meaningful use incentives. Therefore, the criteria for meaningful use are an important defining component of the functional requirements in developing statewide exchange. This section summarizing an analysis of the meaningful use criteria, as outlined by CMS in the draft rule. It is separated into functional requirements, which are derived from the criteria itself, and technical requirements, which are the technical components of a solution that must be created or supported in order to meet the function requirements.

2.1.1 Functional Requirements Analysis

The draft rule calls out 25 criteria for meaningful use of EHR technology. Of these, 13 have been identified as requiring HIE or significantly benefiting from HIE:

1) Use e-prescribing where permissible
2) Incorporate structured lab results
3) Check eligibility electronically
4) Submit claims electronically
5) Provide patients with an electronic copy of their health information
6) Provide patients with online access
7) Exchange information among patient-authorized providers or entities
8) Provide summary of care for transitions and referrals
9) Submit data to immunization registries
10) Submit lab results to public health
11) Submit surveillance data to public health
12) Report aggregated quality data to CMS
13) Perform medication reconciliation

Of the 13 criteria listed above, the last – perform medication reconciliation – is not always included among those requiring or benefiting from HIE. The primary reason is that the information required for medication reconciliation is usually included in other clinical information already exchanged to support transitions of care – a criterion already included in the list – and that the act of reconciliation itself is provided by an EHR, not HIE. It is included in this analysis in order to identify any specific requirements associated with the exchange of medication information to support medication reconciliation.

Most agree that the following meaningful use criteria can be implemented by EHRs or other technologies without the need or requirement for HIE:

14) Record demographics
15) Record vital signs

16) Record smoking status
17) Perform drug-drug, drug-allergy, drug-formulary checks
18) Use electronic order entry
19) Maintain an active medication list
20) Maintain an active allergy list
21) Maintain problem list of active diagnoses
22) Provide clinical summary for office visits
23) Send reminders to patients
24) Generate listings of patients with specific conditions
25) Use decision support relevant to quality metrics

Finally, the meaningful use criteria also require security risk analysis be performed on all HIT initiatives.

Table 1 below provides a more detailed analysis of the 13 meaningful use criteria that require or might benefit from HIE capabilities. For each criterion, the table lists the criterion, the relevant HIE capability that may help providers in meeting that criterion, and the functional requirements for that criterion.

Table 1 Summary of functional requirements derived from the meaningful use criteria published in the draft rule.

Meaningful Use Criteria	Relevant HIE Capability	Functional Requirements
1. Generate and transmit permissible prescriptions electronically	Infrastructure for an EHR or EHR module to correctly address and securely transmit an electronic prescription to the desired dispensing pharmacy in the specified standard format. The Transmission may occur directly or via a third party.	• Network location of receiving entities (i.e., pharmacies) • Authentication of exchanging entities • Secure information submission
2. Incorporate clinical lab-test results into EHR as structured data	Infrastructure for labs to securely transmit structured lab results to the EHR or EHR module of the appropriate provider(s) in the specified standard format. The transmissions may occur directly between labs and EHRs or via a third party.	• Network location of receiving entities (i.e., provider systems) • Authentication of exchanging entities • Network location of receiving providers • Secure information submission

Meaningful Use Criteria	Relevant HIE Capability	Functional Requirements
3. Check insurance eligibility electronically from public and private payers	Infrastructure to securely query a payer, either manually via a web browser or automatically via EDI, in the specified standard format and to receive an electronic response, either via a web browser or automatically via EDI, in the specified standard format. These transactions may occur directly between providers and payers or via a third party.	• Network location of queried entities (i.e., public and private health plans) • Authentication of exchanging entities • Identity of patients in queried system • Secure query/response exchange
4. Submit claims electronically to public and private payers	Infrastructure to securely transmit claims from a provider organization to a payer in the specified standard format. These transactions may occur directly between providers and payers or via a third party.	• Network location of receiving entities (i.e., public and private health plans) • Authentication of exchanging entities • Secure information submission
5. Provide patients with an electronic copy of their health information / discharge instructions upon request	HIE capability is required if the electronic copy is transmitted to the patient via a network, either directly (e.g., via secure email) or through a third-party patient-authorized entity (e.g., a PHR). In these cases, the capability is required to correctly address and securely transmit the information in an accepted format to the patient or the patient-authorized entity.	• Network location of queried and/or receiving entities (i.e., PHRs, providers systems) • Authentication of exchanging entities • Identity of patients in queried and/or receiving system • Secure query/response exchange and/or information submission
6. Provide patients with timely electronic access to their health information within 96 hours	HIE capability is required if electronic access is provided to patients via a third-party patient-authorized entity, such as an “untethered” PHR or secure messaging service.	• Network location of queried entities (i.e., PHRs) • Authentication of exchanging entities • Identity of patients in queried system • Secure query/response exchange

Meaningful Use Criteria	Relevant HIE Capability	Functional Requirements
7. Capability to exchange key clinical information among providers of care and patient-authorized entities electronically	Infrastructure to correctly address and securely transmit the specified types of information (problem list, medication list, etc.) in an acceptable data format from one provider to another, from a provider to a patient-authorized entity, or from a patient-authorized entity to a provider.	• Network location of receiving or queried entities (i.e., provider systems) • Authentication of exchanging entities • Network location of receiving providers • Identity of patients in queried and/or receiving system • Secure query/response and/or information submission
8. Provide summary-of-care record for each transition of care and referral	HIE capability is required if (1) the transition of care or referral is made to a different organization and (2) if the summary-of-care record is communicated in electronic format over a network. In this case, the capability is required to correctly address and securely transmit the record to the new or referred site of care in a specified data format.	• Network location of receiving entities (i.e., provider organizations) • Authentication of exchanging entities • Network location of receiving providers • Identity of patients in queried or receiving system • Secure query/response and/or information submission
9. Capability to submit electronic data to immunization registries and actual submission where required and accepted	Infrastructure to securely transmit immunization events from any hospital or outpatient facility to the appropriate immunization registry for the appropriate patient in a specified data format	• Network location of receiving entities (i.e., immunization registries or public health departments) • Authentication of exchanging entities • Identity of patients in receiving system • Secure information submission

Meaningful Use Criteria	Relevant HIE Capability	Functional Requirements
10. Capability to provide electronic submission of reportable lab results to public health agencies and actual submission where it can be received	Infrastructure to securely transmit lab results from any hospital laboratory to the appropriate public health agency in a specified standard format (including required de-identification of the data)	• Network location of receiving entities (i.e., public health departments) • Authentication of exchanging entities • Secure information submission
11. Capability to provide electronic syndromic surveillance data to public health agencies and actual transmission according to applicable law and practice	Infrastructure to securely transmit relevant clinical data from any hospital or outpatient facility to the appropriate public health agency in a specified standard format (including required de-identification of the data)	• Network location of receiving entities (i.e., public health departments) • Authentication of exchanging entities • Secure information submission and/or information feed
12. Report ambulatory quality measures to CMS or states	Accurate generation of ambulatory quality measures may require the electronic aggregation of clinical data from multiple organizations (as above). In this case, the same HIE capability is required as for #12 above.	• Network location of receiving entities (i.e., CMS) • Authentication of exchanging entities • Secure information submission • Secure exchange over NHIN
13. Perform medication reconciliation at relevant encounters and each transition of care	Accurate medication reconciliation may require the electronic aggregation of medication data from multiple organizations where care was received or medications dispensed.	• Network location of queried entities (i.e., pharmacies, provider organizations, registries, etc) • Authentication of exchanging entities • Identity of patients in queried system • Secure query/response exchange

2.1.2 Technical Requirements Analysis

What is clear from the analysis of functional requirements derived from the meaningful use criteria is that there is a great deal of commonality various criteria. This section includes a high-

level analysis of the functional requirements themselves, traceable to meaningful use criteria supported as a result of the information in Table 1, and the technical components and/or standards requirements derived from them.

Table 2 collects all of the functional requirements found in the in Table 1,

Table 2 Summary of technical requirements derived from the functional requirements of the meaningful use criteria published in the draft rule.

Functional Requirement	Technical Requirement	Supported Meaningful Use Criteria
Secure information submission	• Standards-based message framework for secure and reliable exchange • Trust framework for authorization and consumer consent • Standards-based service specification for submitting information (push exchange pattern)	• e-prescribing • lab results delivery • claims submission • provide copies to patients • exchange among providers • summary at care transition • submit immunizations • public health reporting • public health surveillance • reporting quality measures
Secure query/response exchange	• Standards-based message framework for secure and reliable exchange • Trust framework for authorization and consumer consent • Standards-based service specification for query and response exchange pattern	• eligibility verification • provide copies to patients • provide patient access • exchange among providers • summary at care transition • medication reconciliation
Secure information feeds	• Standards-based message framework for secure and reliable exchange • Trust framework for authorization and consumer consent • Standards-based service specification for information feeds (e.g., publish and subscribe exchange pattern)	• public health surveillance
Secure exchange over NHIN	• NHIN gateway	• reporting quality measures

Functional Requirement	Technical Requirement	Supported Meaningful Use Criteria
Authentication of exchanging entities	• Digital certificate authority with appropriate provisioning and revocation procedures • Standards-based service interface to certificate authority	• e-prescribing • lab results delivery • eligibility verification • claims submission • provide copies to patients • provide patient access • exchange among providers • summary at care transition • submit immunizations • public health reporting • public health surveillance • reporting quality measures • medication reconciliation
Network location of entities receiving information or queries for information	• Entity directory with appropriate procedures for provisioning entities, including o provider organizations, o pharmacies, o labs, o public and private health plans, o patient-authorized entities (e.g., PHRs), and o public health departments • Standards-based service interface to entity directory	• e-prescribing • lab results delivery • eligibility verification • claims submission • provide copies to patients • provide patient access • exchange among providers • summary at care transition • submit immunizations • public health reporting • public health surveillance • reporting quality measures • medication reconciliation
Network location of providers receiving information	• Provider directory with appropriate procedures for provisioning providers • Standards-based service interface to provider directory	• lab results delivery • exchange among providers • summary at care transition
Identity of patients in the system being queried and/or receiving information	• Standards-based service specification for agreeing on patient identities	• eligibility verification • provide copies to patients • provide patient access • exchange among providers • summary at care transition • submit immunizations • medication reconciliation

The above analysis identifies a set standards-based technical and service specifications and a set of software components that are required to support the 13 meaningful use criteria that either require or can benefit from HIE. The technical specifications include:

Table 3 Summary of required technical specifications derived from meaningful use criteria.

1	a standards-based message framework for secure and reliable health information exchange
2	a trust framework for authorization and consumer consent
3	a standards-based service interface to a root certificate authority that “authenticates” an entity
4	a standards-based service interface to a directory of all entities participating in exchange
5	a standards-based service interface to a directory of providers participating in exchange
6	a standards-based service specification for discovering patient identities and agree on shared identities
7	a standards-based service specification for (1) a push exchange pattern, (2) a query and response exchange pattern, and (3) a publish and subscribe exchange pattern

Some of these specifications are supported by required software components. Key among them are:

Table 4 Summary of required key software components derived from meaningful use criteria.

1	a digital certificate authority that is supported by a standards-based interface and supporting the messaging framework and trust framework
2	a directory of entities participating in exchange, including provider organizations of various sizes, chain and independent pharmacies, labs, public and private health plans, other patient authorized entities such as PHRs or patient-controlled health records (PCHRs), and public health departments and systems, supported by a standards-based interface and supporting the messaging framework
3	a directory of providers participating in exchange, which might be centralized or federated and is supported by a standards-based interface
4	a gateway interface to the Nationwide Health Information Network

A number of these software components and service specifications are included in NHIN and are discussed further in Section 2.2 *Nationwide Health Information Network Services and Standards* below.

While not required to achieve meaningful use, a number of higher-level value-added services have also been identified and might be included in a statewide exchange. Table 5 below outlines some value-added services that have been identified.

Table 5 Summary of high-level value-added services that are not required for meaningful use, but might have value to stakeholders.

Meaningful Use Criteria	Potential Value-added Functionality
• Lab results delivery • Public health reporting • Public health surveillance	Translation service that facilitates translating structured lab results into standard format(s)
	Clearinghouse as a single delivery point for lab systems that facilitates routing of lab results to appropriate provider systems and/or public health departments
• Eligibility verification	Clearinghouse as a single access point for EHRs and practice management systems for insurance eligibility information via EDI transactions across various health plans
• Provide copies to patients • Provide patient access	Widespread secure messaging system to enable patients and providers to communicate electronically.
• Exchange among providers • Summary at care transition	Translation service that facilitates translating and transforming among standardized summary clinical formats.
	Clearinghouse as a single delivery point for EHRs for routing clinical summary documents among providers and patient-designated entities.
• Submit immunizations	Clearinghouse as a delivery point that can accept immunization messages from EHRs and forward them to the intended immunization registry.
• Public health reporting • Public health surveillance	Utility service to manage pseudonymization and re-identification when required.

Many of these services would depend upon the standards-based service specifications and software components outlined in Table 2. They may also relieve providers of some of the IT complexity in realizing important business processes, and therefore constitute potential revenue for statewide shared services.

2.2 Nationwide Health Information Network Services and Standards

The Nationwide Health Information Network is a set of services, standards, and policies being developed by ONC that enable secure exchange of health information over the Internet to connect providers, consumers, and others involved in supporting health and healthcare. Secure exchange over the NHIN is accomplished through a small set of infrastructure components, a legal agreement among exchange partners called the Data Use and Reciprocal Support Agreement (DURSA), and a set of web-service specifications that define a framework for messaging, authorization, patient consent, discovery, and exchange.

A group of federal agencies, local, regional and state-level HIOs and integrated delivery networks, formerly known as the NHIN Cooperative, has been helping to develop the NHIN standards, services, and policies. Today, these organizations are demonstrating live health information exchange through the NHIN Exchange[2]. By the end of 2010, ONC expects that approximately a dozen entities will be securely sharing live health information as part of this Exchange.

NHIN is now in its third phase, termed Limited Production Exchange. In order to participate in Exchange, organizations must go through the "on-boarding" process which entails:

1) completing an application for participation, available only through a sponsoring federal agency;
2) executing a trust agreement called the Data Use and Reciprocal Support Agreement (DURSA);
3) completing required technical testing / validation procedures; and
4) been accepted by an NHIN Coordinating Committee, which supports operation of the NHIN Limited Production Exchange.

2.2.1 Exchange with Federal Agencies and Other State Initiatives

Today, the NHIN Exchange connects a diverse set of federal agencies and private organizations that need to securely exchange electronic health information. These entities currently include the Social Security Administration, MedVirginia, the Department of Veterans Affairs, the Department of Defense, and Kaiser Permanente.

At this time, non-federal entities can only participate in the Exchange through a federally-sponsored contract that pertains to NHIN implementation. NHIN-related contracts currently include:

- the Social Security Administration (SSA), which just awarded contracts to 15 organizations to expand its pilot with MedVirginia for exchange of medical information to support applications for disability benefits;
- the Virtual Lifetime Electronic Record (VLER), a program currently limited to the Veterans Administration (VA), Department of Defense (DoD), and Kaiser Permanente which is creating a virtual longitudinal record as part of the Wounded Warrior program for military personnel that spans active duty, care in the VA, and care in the private sector;
- the Beacon Communities program, a program that has just announced recipients of 15 awards of funding to strengthen existing HIT infrastructure and exchange capabilities in some key focus areas;
- State HIE Cooperative Agreements that will support the development of statewide health information exchange capabilities;

---

[2] ONC has begun to use the terms "NHIN Exchange" and "Exchange" to differentiate NHIN from NHIN Direct, a new project recently launched by ONC and described later in this document.

- exchange of surveillance information with the Centers for Disease Control and Prevention (CDC), currently focused on H1N1; and
- other emerging federal programs that focus on the NHIN Exchange.

Federal agencies are assessing and prioritizing their rollout strategy and will prioritize their expansion over the next 12 to 18 months. It is clear that the federal agencies will use NHIN Exchange moving forward. Organizations such as the DoD, VA, and CDC are moving away from previous solutions for health information exchange to utilize Exchange instead. CMS has at least four initiatives in conceptual or pilot stages that will utilize NHIN as a preferred method of electronic exchange – one of them the receipt of aggregated quality measures, a meaningful use criteria.

ONC has stated that it expects a significant portion of the funds available through the State HIE Cooperative Agreements Program to be used to facilitate exchange with federal agencies and other states. At this time, it would appear that NHIN Exchange is the preferred mechanism for exchange with federal agencies. Given ONC's requirement, NHIN Exchange may well become the preferred mechanism for exchange with other states as well as other states may be developing NHIN capabilities as well.

Therefore, it may be appropriate to include full technical capabilities to participate in NHIN Exchange as a requirement for statewide exchange.

In addition to considerations to participate in NHIN Exchange, the services and standards for NHIN might be considered examples of nationwide standards for exchange that are part of requirements under the State HIE Cooperative Agreement Program, and provide an example of standards that might be considered for similar services required within the state.

2.2.2 NHIN Messaging Framework

Key to NHIN is developing a trust framework for the exchange of health information. The trust framework comprises:

1) a standards-based message framework based on SOAP web services and TLS encryption for secure and reliable health information exchange;
2) a trust framework for authorization and consumer consent described in more detail below;
3) a standards-based service interface to a root certificate authority that "authenticates" an entity; and
4) a standards-based service interface to a directory of all entities participating in exchange based on the Universal Description Discovery and Integration (UDDI) standard.

These capabilities are supported by software components that include:

1) a digital certificate authority; and
2) a directory of entities participating in exchange – a database based on UDDI.

Authorization within NHIN is based on the concept of local autonomy – each entity participating in exchange makes its own independent decisions on whether to provide requested information. It is described by two documents: the NHIN Authorization Framework Specification and the NHIN Access Consent Policies Specification.

Figure 1 below illustrates how authorization and patient consent works within the NHIN trust model. Every request for information is made based on a role of the requestor and the purpose-for-use of the request. The role and purpose-for use are carried in a Security Assertion Markup Language (SAML) assertion –an XML-based standard for exchanging authentication and authorization data –that accompanies the request. The organization that receives the request examines the role and purpose-for-use and releases the information if and only if it conforms with its own local policy for disclosure of health information. The policy check would normally also include a check of the consent preferences of patients as known to the local entity.

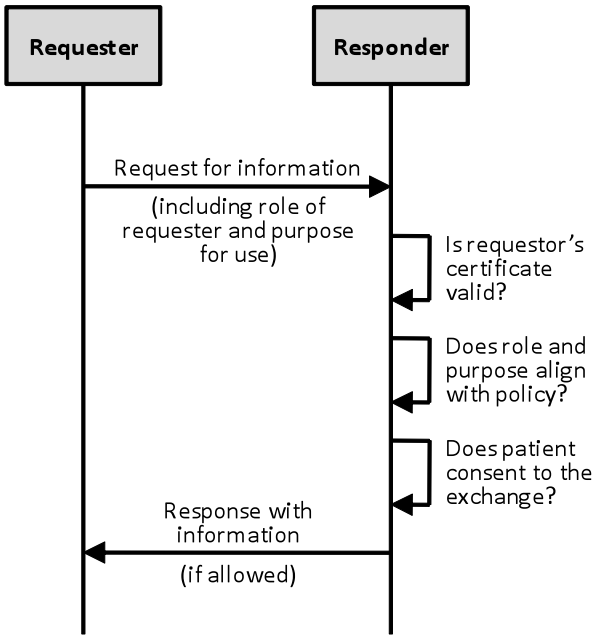

Figure 1 Illustration of the authorization and patient consent solution implemented by NHIN Exchange.

The NHIN trust framework does not require any centralized consent registry or uniform policy for the disclosure of health information. Instead, it is dependent upon local policy of the disclosing organization, and patient preferences for consent known to that organization. This approach allows autonomous organizations to implement disclosure policies that meet the needs of their stakeholders. It also allows patients to consent to disclosure using different rules depending upon the sensitivity of the information present within different organizations.

2.2.3 NHIN Web Services

NHIN Exchange comprises a set of services, standards, and policies for the exchange of information. Key among these are a set of standardized discovery and exchange services that are supported by NHIN participants to facilitate exchange. The following sections describe service specifications that achieve:

1) discovering entities participating in NHIN exchange;
2) discovering patient identities and agreeing on shared identities.; and
3) exchange mechanisms for:
   a) a push exchange pattern,

b) a query / response exchange pattern, and
c) a publish / subscribe exchange pattern.

2.2.3.1 Discovery Services

Service Discovery

As described above, NHIN utilizes a software component based on UDDI to act as a directory for entities participating in NHIN exchange. The interface to the UDDI directory is described in the NHIN Web Services Registry Web Service Interface Specification. The service allows one entity to locate the address or "end point" to the web services of others, based on searches that might include the service type, organization's name, state in which the organization is located, or perhaps the type of organization (such as public health agency or Medicaid agency).

Patient Discovery

In order to share patient data within and among entities, it is necessary to have mechanisms to match patient identities in the absence of a single national identifier. The Patient Discovery service meets this need by providing the ability for one entity to determine whether other entities have records for a given patient by submitting a set of demographic identifiers that can be used to match against their own master patient indices.

The transactions implemented by the Patient Discovery service are based on the IHE profile for Cross-Community Patient Discovery (XCPD) and are described in the NHIN Patient Discovery Web Service Interface Specification. The actions are illustrated in Figure 2 below. Patient Discovery is an arbitrated conversation between two or entities, in which a querying entity submits a query to one or more others that its patient ID and demographic information about the patient as it is known to it. Queried entities search their patient indexes for matches. If a match is found, and sharing that patient ID over the NHIN with the other entities is allowed by policy and patient preferences, the its sends its patient ID and the demographic information as it is known to it back to the querying entity. A match is declared if and only if both entities agree on the match.

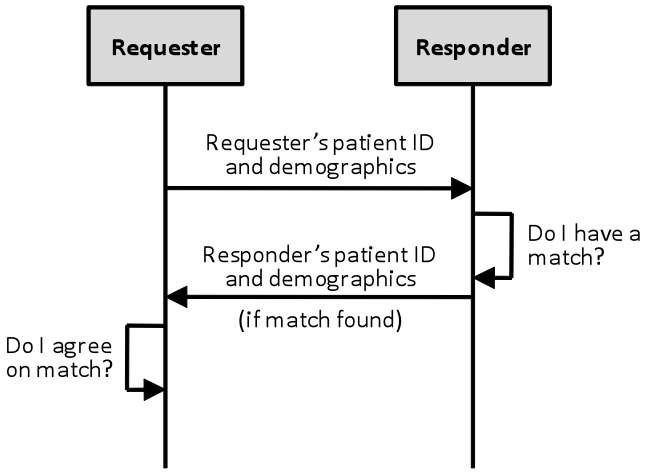

Figure 2 Illustration of the Patient Discovery service implemented by NHIN Exchange.

When queried for a match, an entity can return one of three responses: a match with a patient ID and demographics, a message that there was an ambiguous match and request additional information that might result in a single matching patient, or no match. The latter condition might result from a failure to identify any matches, an ambiguous match, or a failure to meet the authorization requirements of policy or patient preferences.

Importantly, Patient Discovery is a conversation between two entities to reach an agreement on a matching patient. In order for there to be a match, and for exchange to proceed, both entities must agree that the patient is a match, even if they utilize different matching rules internally.

Patient Discovery does not require any centralized master patient index or any national identifier. It also requires no centralized service in order to arrive at matches, but is a specification for how two or more entities would arrive at a match.

2.2.3.2 Exchange Service Patterns

NHIN is technically agnostic to the type of information exchanged, but normally uses a document information model. Therefore, most of the exchange services describe information in terms of documents.

Query and Response Exchange Pattern

The query and response exchange pattern is achieved through two-step process implemented as two separate services: Query for Documents and Retrieve Documents.

The Query for Documents service allows one entity to locates electronic health information on the NHIN associated with a specific patient, normally discovered through Patient Discovery. A query returns a list of documents for a given patient based on a set of search criteria. The transactions implemented by the Query for Documents service are described by the IHE profile for Cross Gateway Query (XCA) and the NHIN Query for Documents Web Service Interface Specification.

The Retrieve Documents service allows an entity to retrieve documents from the list returned by Query for Documents. The transactions implemented by the Retrieve Documents service are likewise described by the IHE profile for Cross Community Access (XCA) and the NHIN Retrieve Documents Web Service Interface Specification.

The XCA specification has been relaxed within the NHIN to support the query for, and retrieval of, dynamically generated document content.

Figure 3 illustrates the query and response exchange pattern. Query for Documents and Retrieve Documents both require the unique patient identifier of the entity providing the data. As a result, it is often preceded by Patient Discovery, but the patient identifier can be obtained by other means. One entity requests a list of documents meeting certain search criteria – such as date, type of document, etc – from another using the patient identifier. The queried entity examines its policies for disclosing information and patient consent preferences against the role and purpose-for-use in the request, and returns a list of any documents that meet the search criteria if and only if allowed by policy. The first entity examines the list, and requests documents on the list for review.

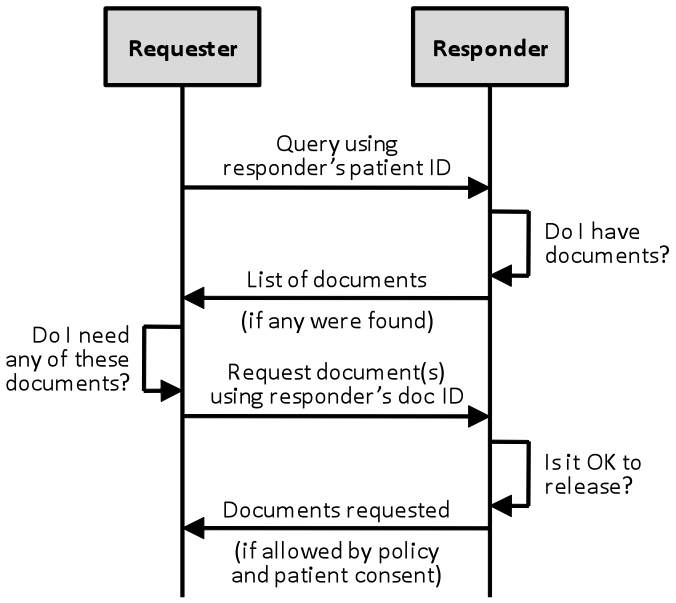

Figure 3 Illustration of the Query for Documents and Retrieve Documents services that implement the query/response exchange pattern in NHIN Exchange.

In this context, a "document" refers to the form of electronic health information as it is transferred between entities not as it is stored within systems such as EHRs in that entity. Any participating system may store health information in whatever format or repository it chooses, so long as it can respond to queries and to retrieve document requests. The primary expected use in the context of the NHIN is that these documents are formatted as XML data following the HL7 Clinical Document Architecture (CDA) standard, but nothing precludes this interface from being used to query for other kinds of documents.

Entities that generate documents dynamically on demand must ensure that the generated document remains available, unaltered, once a document has been retrieved once. This means that entities or systems that generate dynamic documents must retain those documents for some period of time.

Publish and Subscribe Exchange Pattern

Health Information Event Messaging, or HIEM, refers to the NHIN specification for a publish and subscribe exchange pattern. HIEM is an extension to the OASIS Web Services Base Notification 1.3 (WS-BaseNotification) utilizing Web Services Topics 1.3 (WS-Topics), and is described in the NHIN Health Information Event Messaging Web Service Interface Specification.

There are two primary workflows involved in HIEM: an entity-initiated subscription to receive a feed of information from another entity, and a notification that information conforming to that subscription is available ("has been published"). Both are illustrated in Figure 4 below. The subscription may specify what type of information is desired, how often, etc. It must contain a role and purpose-for-use that the publishing organization will use to determine whether the disclosure of information is allowed by policy and by the patient preferences for consent.

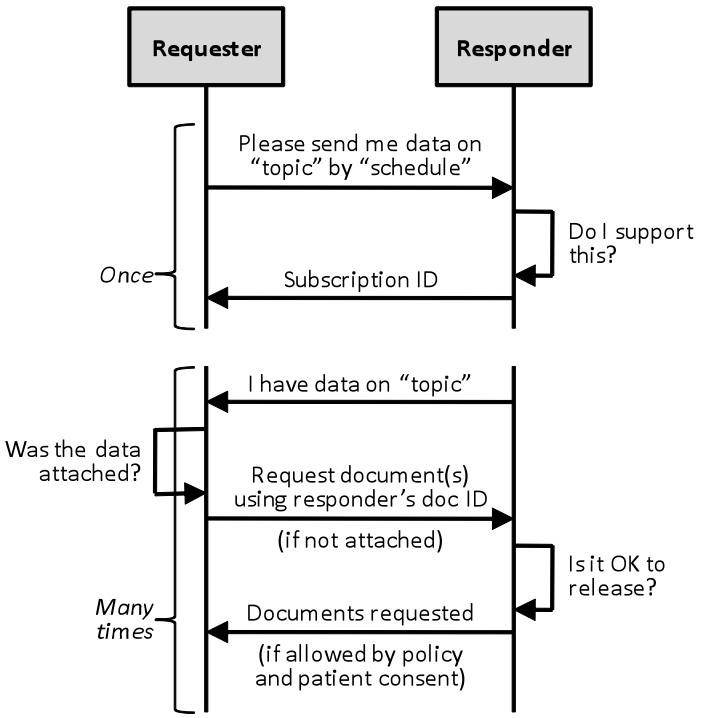

Figure 4 Illustration of the information feed exchange pattern implemented by the Health Information Event Messaging service in NHIN Exchange.

The HIEM model is a form of query and response in which the query is made once, and responses are sent when data is available. The responses may be of two types: they may contain the requested health information, or they may include a pointer to a document that contains the information. In the latter case, Retrieve Documents can be used to retrieve a copy of that document.

HIEM is intended to be used when continuous feeds of information are desired, and therefore continuing Query for Documents is inappropriate. Since it is initiated with a subscription, the type and frequency for which the data is returned is under the control of the subscribing organization, and the feed can be altered or discontinued as desired. This is in contrast to the push exchange mechanism, where a feed might be established due to policy, but there is no electronic method to alter or discontinue it. Within the NHIN community, HIEM is though appropriate for syndromic surveillance, where a public health agency might alter feed frequency during an outbreak or during flu season. The push exchange pattern might be more appropriate for mandatory public health reporting that is prescribed by law and unlikely to change frequently.

Push Exchange Pattern

The Document Submission service allows an entity to send documents to another without a corresponding electronic request. The transactions implemented by the Document Submission service are described by the IHE profile for Cross-Enterprise Document Reliable Interchange (XDR) and the NHIN Document Submission Web Services Interface Specification draft, not yet released.

The Document Submission service provides the ability for one organization to "push" identified health information for a given patient from one entity to another, triggered by events at the submitting organization. It might be used, for example, to deliver lab results electronically when the order was received by paper, or to submit quality measures on a prescribed schedule. Document Submission provides a different model of exchange than the publish and subscribe model implemented by HIEM, as the sending entity determines what entities should receive the information and what information to send.

Figure 5 illustrates the simple push transaction implemented by Document Submission.

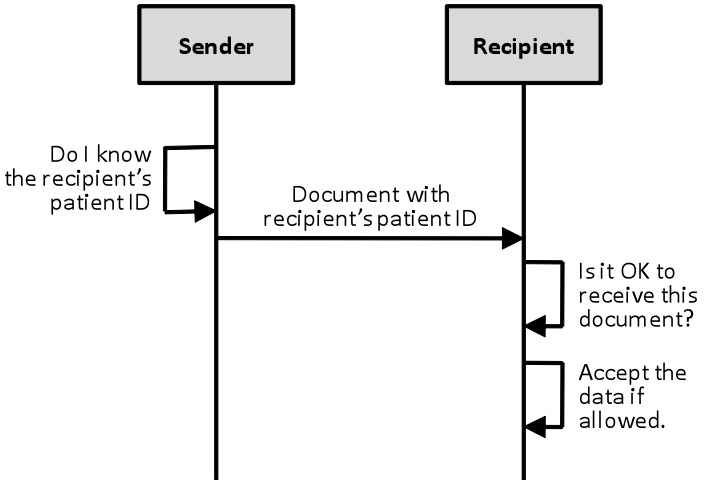

Figure 5 Illustration of the Document Submission service that implement the unsolicited submission exchange pattern in as an emerging standard for NHIN Exchange.

Document Submission normally requires that the patient identifier of the receiving entity be know, and therefore the Document Submission service may be used in conjunction with the Patient Discovery service to retrieve the patient ID of matching patients. It may also be used without Patient Discovery when the patient identifier is known by other means. For example, a lab order may include identifying information that allows a lab to send results via Document Submission with a patient identifier without the need for Patient Discovery.

2.2.3.3 Content Standards

As stated earlier, NHIN is technically content agnostic; it is capable of exchanging any information that conforms to the SOAP web services standard for messaging. The SOAP standard calls for information to be encapsulated in XML documents.

However, NHIN conventions suggest that the health information should conform to the HL7 Clinical Document Architecture standard, which is part of HL7 v3 consistent with the Reference Information Model (RIM). The Healthcare Information Technology Standards Panel[3] (HITSP)

---

3 As of this writing, HITSP has ceased operations under its contract with ONC. However, the HITSP web site is till operational at http://www.hitsp.org.

defined a relatively large number of documents conforming to the CDA standard to meet various uses in health information exchange. NHIN profiles – descriptions of how services are put together to fulfill specific business processes – make heavy use of HITSP-defined CDA document types.

2.2.4 Summary of NHIN Services and Standards

Table 6 below provides summary of the services and standards specifications for NHIN.

Table 6 Summary of the discovery and exchange services and standards that are implemented by NHIN Exchange.

Service	Description	HITSP Specification or IHE Profile	Other Standards
Patient Discovery	The first in a three-step process which defines the query/retrieve exchange pattern, Patient Discovery is an arbitration process that allows two organizations to agree on matching patient IDs based on exchanged demographic information. Patient Discovery can also be used outside of the query/retrieve exchange pattern to discover the patient ID in another organization.	IHE Cross-community Patient Discovery (XCPD)	HL7 v3 Patient Administration DSTU, Patient Topic
Web Services Registry	The Web Services Registry service allows organizations to discover nodes on the NHIN and retrieve service connection information. Currently, organizations can be located based on their home community ID or by their home state.		OASIS Universal Discovery and Description Interface (UDDI)
Query for Documents	The second in a three-step process which defines the query/retrieve exchange pattern, Query for Documents allows an organization to discover existing documents, optionally meeting specific search criteria, for a patient located by the Patient Discovery service.	HITSP TP13 Manage Sharing of Documents Transaction Package IHE Cross-community Access (XCA)	

Service	Description	HITSP Specification or IHE Profile	Other Standards
Retrieve Documents	The third in a three-step process which defines the query/retrieve exchange pattern, Retrieve Documents allows an organization to retrieve documents discovered by the Query for Documents service.	HITSP TP13 Manage Sharing of Documents Transaction Package IHE Cross-community Access (XCA)	
Health Information Event Messaging (HIEM)	HIEM defines a generic publish and subscribe mechanism that can be used to initiate feeds of information (publication) from one or more organizations that is initiated and controlled (subscription) by an organization. Various NHIN Profile Definitions outline how HIEM may be used to achieve specific objectives.		OASIS WS-BaseNotification OASIS WS-Topics
Document Submission	An emerging specification which defines the unsolicited document submission exchange pattern, Document Submission allows an organization to send an expected document to another without requiring a request, perhaps for a patient located by Patient Discovery.	IHE Cross-enterprise Document Reliable Interchange (XDR)	

2.2.5 NHIN Coverage of Meaningful Use Requirements

Section 2.1.2 *Technical Requirements Analysis* identified a set standards-based technical and service specifications derived from the 13 meaningful use criteria that require or can benefit from HIE. Table 7 lists those specifications, and identifies those that are addressed by NHIN Exchange.

Table 7 List of technical specifications derived from meaningful use criteria that are met by NHIN Exchange.

√	1	a standards-based message framework for secure and reliable health information exchange
√	2	a trust framework for authorization and consumer consent
√	3	a standards-based service interface to a root certificate authority that “authenticates” an entity

√	4	a standards-based service interface to a directory of all entities participating in exchange
	~~5~~	~~a standards-based service interface to a directory of providers participating in exchange~~
√	6	a standards-based service specification for discovering patient identities and agree on shared identities
√	7	a standards-based service specification for (1) a push exchange pattern, (2) a query and response exchange pattern, and (3) a publish and subscribe exchange pattern

Likewise, Section 2.1.2 *Technical Requirements Analysis* identified a set of required software components derived from the 13 meaningful use criteria that require or can benefit from HIE. Table 8 lists those components, and identifies those that are addressed by NHIN Exchange.

Table 8 List of technical specifications derived from meaningful use criteria that are met by NHIN Exchange.

√	1	a digital certificate authority that is supported by a standards-based interface and supporting the messaging framework and trust framework
√	2	a directory of entities participating in exchange, including provider organizations of various sizes, chain and independent pharmacies, labs, public and private health plans, other patient authorized entities such as PHRs or patient-controlled health records (PCHRs), and public health departments and systems, supported by a standards-based interface and supporting the messaging framework
	~~3~~	~~a directory of providers participating in exchange, which might be centralized or federated and is supported by a standards-based interface~~
√	4	a gateway interface to the Nationwide Health Information Network

2.3 NHIN Direct Services and Standards

Based on initial recommendations from the NHIN Work Group of the HIT Policy Committee, a new initiative was launched to explore the NHIN standards and services required to enable secure health information exchange at a more local and less complex level, such as a primary care provider sending a referral or care summary to a local specialist electronically. This initiative is known as NHIN Direct[4].

Organizationally, NHIN Direct is a set of volunteers with staff support from ONC. A core set, known as the Implementation Group, meet weekly by phone to discuss and reach consensus on

[4] ONC continues to refer to this initiative as the "NHIN Direct Project" rather than NHIN Direct in official publications rather than "NHIN Direct".

standards and services for the NHIN Direct project. Work products are posted on a wiki at http://www.nhindirect.org, where anyone can comment or contribute. Additionally, the Implementation Group has agreed to create a reference implementation of the services.

2.3.1 NHIN Direct Web Services

NHIN Direct was initiated in March 2010, and has not yet defined a set of services and standards. If has focused on an expanding set of use cases that currently include:

1) Primary care provider refers patient to specialist including summary care record.
2) Primary care provider refers patient to hospital including summary care record.
3) Specialist sends summary care information back to referring provider.
4) Hospital sends discharge information to referring provider.
5) Laboratory sends lab results to ordering provider.
6) Transaction sender receives delivery receipt.
7) Provider sends patient health information to patient.
8) Hospital sends patient health information to patient.
9) Provider sends clinical summary of office visit to patient.
10) Hospital sends clinical summary at discharge to patient.
11) Provider sends reminder for preventive or follow-up care to patient.
12) Primary care provider sends patient immunization data to public health.

What is key from this list is that NHIN Direct focuses on a push service model that delivers health information, most often between providers or provider organizations. NHIN Direct does not include a query and response mechanism – there is no way to request information over NHIN Direct – or discovery services to identify patients, providers, or organizations.

NHIN Direct differs from NHIN Exchange in that the latter is defined as an exchange among organizations, while NHIN Direct reaches to individual providers or patients. As a result, NHIN Direct is defining not only a set of services and standards to support them, but also an addressing scheme for identifying which provider is the ultimate target recipient of information. This capability, at this point, does not appear to include a directory of providers. In fact, NHIN Direct is sometimes defined as a set of services, standards, and policies for secure exchange of health information over the Internet *with someone you know*.

NHIN Direct working groups are considering a number of approaches to addressing, including a model based on email addresses which is receiving the most traction, or REST[5] or other web service addresses. It may use simple mail transport protocol (SMTP), RESTful web services, or an IHE profile for transport. Again, SMTP is getting the most traction in conjunction with email-style addressing.

2.3.2 Role of NHIN Direct

NHIN Direct seeks to expand the standards and service definitions that currently constitute the NHIN. Those standards and services will allow organizations to deliver simple, direct, secure and scalable transport of health information over the Internet between known participants in

---

5 Representational State Transfer (REST) is an architecture for web services considered lighter weight than SOAP, utilizing the core GET and PUT structures of HTTP utilized by web browsers, rather than the remote procedure call structure of SOAP. Conforming to the REST constraints is referred to as being "RESTful".

support of Stage 1 meaningful use, and provide an easy "on-ramp" for a wide set of providers and organizations looking to adopt. Like NHIN Exchange, the key products of NHIN Direct will be standards and service definitions, implementation guides, reference implementations, and associated testing frameworks.

However, it supports only a push model for information exchange. The project also has explicitly excluded administrative transactions, such as eligibility verification and claims submission, from its consideration, suggesting that these transactions are well-supported by standards and vendors already.

2.3.3 NHIN Direct Coverage of Meaningful Use Requirements

Section 2.1.2 *Technical Requirements Analysis* identified a set standards-based technical and service specifications derived from the 13 meaningful use criteria that require or can benefit from HIE. Table 9 lists those specifications, and identifies those that may be addressed by NHIN Direct.

Table 9 List of technical specifications derived from meaningful use criteria that may be met by NHIN Direct.

√	1	a standards-based message framework for secure and reliable health information exchange
√	2	a trust framework for authorization ~~and consumer consent~~
?	3	a standards-based service interface to a root certificate authority that "authenticates" an entity
	~~4~~	~~a standards-based service interface to a directory of all entities participating in exchange~~
?	5	a standards-based service interface to a directory of providers participating in exchange
	~~6~~	~~a standards-based service specification for discovering patient identities and agree on shared identities~~
√	7	a standards-based service specification for (1) a push exchange pattern, ~~(2) a query and response exchange pattern, and (3) a publish and subscribe exchange pattern~~

Likewise, Section 2.1.2 *Technical Requirements Analysis* identified a set of required software components derived from the 13 meaningful use criteria that require or can benefit from HIE. Table 10 lists those components, and identifies those that may be addressed by NHIN Direct.

Table 10 List of technical specifications derived from meaningful use criteria that may be met by NHIN Direct.

?	1	a digital certificate authority that is supported by a standards-based interface and supporting the messaging framework and trust framework

~~2~~	~~a directory of entities participating in exchange, including provider organizations of various sizes, chain and independent pharmacies, labs, public and private health plans, other patient authorized entities such as PHRs or patient-controlled health records (PCHRs), and public health departments and systems, supported by a standards-based interface and supporting the messaging framework~~
~~3~~	~~a directory of providers participating in exchange, which might be centralized or federated and is supported by a standards-based interface~~
~~4~~	~~a gateway interface to the Nationwide Health Information Network~~

What is evident from Table 9 and Table 10 above is that NHIN Direct has little infrastructure to support secure information exchange and supports only a push exchange model. While it provides a mechanism to address individual providers, it most likely will not include a directory that can be used to locate them.

2.4 Standards for EHR Technology

Successful implementation of HIE is dependent upon the use of recognized HIT standards. To this end, ONC published an Interim Final Rule (IFR) on an initial set of standards, implementation specifications, and certification criteria on December 30, 2009 for adoption by the Secretary of HHS. The IFR represents the first step in what ONC plans as an incremental approach to adopting standards, implementation specifications, and certification criteria to support its meaningful use.

It is expected that the requirement for statewide HIE to utilize recognized nationwide standards as outlined in the State HIE Cooperative Agreements program includes the provisions of the IFR. This section summarizes at a high level the standards requirements of the IFR and contrasts them with NHIN Exchange.

2.4.1 Summary Requirements of the Interim Final Rule

The IFR outlines interoperability standards that extend to content of the information that is transmitted, the vocabulary or coding standard that is to be used in that transmission, the form of the transmission itself, and the privacy and security standards that must be implemented to ensure that the transmission is secure. The following list summarizes some of the most relevant standards guidance in the IFR

2.4.1.1 Information Content Standards

Patient Summary Record

The Patient Summary Record should be represented a continuity of care document (CCD) or continuity of care record (CCR), and converge to a single standard in the near future.

The Continuity of Care Record (CCR) is an XML-based health record standard specification developed jointly by ASTM International, the Massachusetts Medical Society (MMS), the Healthcare Information and Management Systems Society (HIMSS), the American Academy of Family Physicians, the American Academy of Pediatrics, and other health informatics vendors. It is a way to create flexible documents that contain the most relevant and timely core health

information about a patient, created specifically in order to send this infroamtion electronically from one care giver to another. It contains various sections such as patient demographics, insurance information, diagnosis and problem list, medications, allergies and care plan that represent a “snapshot” of a patient's health data.

The Continuity of Care Document (CCD) specification is likewise an XML-based markup standard intended to specify the encoding, structure and semantics of a patient summary clinical document for exchange. The CCD specification is a constraint on the HL7 clinical document architecture (CDA) standard. The CDA specifies that the content of the document consists of a mandatory textual part (which ensures human interpretation of the document contents) and optional structured parts (for software processing). The structured part is based on the HL7 Reference Information Model (RIM). The CCD constraint on the CDA is based on the CCR. Therefore, the CCR and CCD represent similar content using different organizational standards.

The problem list in the CCR or CCD should be represented in ICD-9 (migrating to ICD-10 when mandated) and SNOMED-CT (Systematized Nomenclature of Medicine – Clinical Terms) coding standards. Medications should be represented in RxNorm. There are no standard representations for allergies or vital signs at this time.

e-Prescribing

The content of e-prescribing transactions is dictated by the National Council for Prescription Drug Programs (NCPDP). Drug formulary checks – not specifically part of e-prescribing but usually associated with it – is based on the NCPDP Forumarly & Benefits Standard as well.

Both the script and formulary information should be represented in RxNorm mappings to existing commercial products.

Administrative Transactions

Administrative transactions are defined as those required by Health Insurance Portability and Accountability Act of 1996 (HIPAA). The current version of the standard, version 4010, was scheduled to take effect on 16 October 2003, but was delayed due to widespread confusion and difficulty in implementing the rule. The new version 5010 standard is to becomes effective in 2013, replacing the current 4010 version that, among other things, allows for the larger field size of ICD-10, as well as other improvements.

The HIPAA transaction standards are based on Accredited Standards Committee (ASC) X12, a set of electronic data interchange (EDI) standards that include:

1) Health Care Claim Transaction set (837) – used to submit health care claim billing information, encounter information, or both.
2) Retail Pharmacy Claim Transaction (NCPDP Telecommunications Standard version 5.1) – used to submit retail pharmacy claims to payers by health care professionals who dispense medications, either directly or via intermediary billers and claims clearinghouses.
3) Health Care Claim Payment/Advice Transaction Set (835) – used to make a payment, send an Explanation of Benefits (EOB) remittance advice, or make a payment and send an EOB remittance advice from a health insurer to a health care provider either directly or via a financial institution.
4) Benefit Enrollment and Maintenance Set (834) – used by employers, unions, government agencies, associations or insurance agencies to enroll members to a payer.

The payer is a healthcare organization that pays claims, administers insurance or benefit or product.

5) Payroll Deducted and other group Premium Payment for Insurance Products (820) – a transaction set which can be used to make a premium payment for insurance products. It can be used to order a financial institution to make a payment to a payee.
6) Health Care Eligibility/Benefit Inquiry (270) – used to inquire about the health care benefits and eligibility associated with a subscriber or dependent.
7) Health Care Eligibility/Benefit Response (271) – used to respond to a request inquire about the health care benefits and eligibility associated with a subscriber or dependent.
8) Health Care Claim Status Request (276) – a transaction set can be used by a provider, recipient of health care products or services or their authorized agent to request the status of a health care claim.
9) Health Care Claim Status Notification (277) – a transaction set used by a health care payer or authorized agent to notify a provider, recipient, or authorized agent regarding the status of a health care claim or encounter, or to request additional information from the provider regarding a health care claim or encounter.
10) Health Care Service Review Information (278) – a transaction set used to transmit health care service information, such as subscriber, patient, demographic, diagnosis, or treatment data for the purpose of request for review, certification, notification, or reporting the outcome of a health care services review.
11) Functional Acknowledgement Transaction Set (997) – a transaction set used to define the control structures for a set of acknowledgments to indicate the results of the syntactical analysis of the electronically encoded documents (not specifically named in the HIPAA legislation, but necessary for X12 transaction set processing

The Council for Affordable Quality Healthcare (CAQH) is a nonprofit alliance of health plans and trade associations, working to simplify healthcare administration through industry collaboration on public-private initiatives. Through two initiatives – the Committee on Operating Rules for Information Exchange (CORE) and Universal Provider Datasource (UPD) – CAQH aims to reduce administrative burden for providers and health plans. CAQH Core I guidelines are to be used for implementation guidance of the X12 HIPAA transactions.

Quality Reporting

Quality measures are to be based on the National Quality Forum (NQF) Health Information Technology Expert Panel Definitions. NQF is a nonprofit organization that endorses national consensus standards for measuring and publicly reporting on performance.

Content for quality measures is to be based on the Physician Quality Reporting Initiative (PQRI) standard, an XML-based standard for quality reporting. The format may migrate to use the Quality Reporting Document Architecture (QRDA), a standards development initiative formed to develop an electronic data standard for exchange of patient-level quality measurement data between health care information systems based on the HL7 CDA.

Laboratory Results

Content is to be based on the HL7 version 2.5.1 standard using Logical Observation Identifiers Names and Codes (LOINC) for terminology. LOINC is a universal standard for identifying medical laboratory observations developed and maintained by the Regenstrief Institute. Since

its inception, the database has expanded to include not just medical and laboratory code names, but also: nursing diagnosis, nursing interventions, outcomes classification, and patient care data set.

Public Health Surveillance

Content is to be based on HL7 version 2.3.1 or version 2.5.1 using Geocoded Interoperable Population Summary Exchange (GIPSE). GIPSE, formerly called the Aggregate Minimum Data Set or AMDS, is an XML standard for representation of summary or aggregated, de-identified health information for surveillance purposes.

Immunizations

Content is to be based on HL7 version 2.31 or version 2.51 using CVX, an HL7 external code set developed and maintained by the Center for Disease Control and Prevention's (CDC's) National Immunization Program (NIP).

2.4.1.2 Information Transmission Standards

The IFR calls for the exchange of information using web services over the Internet. Two separate standards for web services are listed: SOAP version 1.2 and REST, both described in more detail below.

SOAP

SOAP was originally defined as the Simple Object Access Protocol, but the acronym was dropped with version 1.2 of the standard. SOAP a protocol specification developed and maintained by the World Wide Web Consortium (W3C) for exchanging structured information web services. It relies on eXtensible Markup Language (XML) as its message format, and usually relies on other application layer protocols (most notably Remote Procedure Call and HTTP) for message negotiation and transmission.

SOAP messages consist of three parts:

1) an envelope which defines what is in the message and how to process it;
2) a set of encoding rules for expressing instances of application-defined datatypes; and
3) a convention for representing procedure calls and responses.

SOAP web services follow a remote-procedure-call method for web services, similar in concept to function calls in more traditional programming. It is very flexible and powerful, but is thought by some to be relatively heavy to implement and requiring a great deal of data in XML format to implement.

Within the IFR, SOAP is to use Hypertext Transfer Protocol (HTTP) for transport.

REST

Representational State Transfer (REST) is a style of software architecture for distributed hypermedia systems such as the World Wide Web. The REST architectural style was developed in parallel with the HTTP version 1.1 protocol. The World Wide Web is an example of the REST architectural style, which might in fact be considered a *post hoc* description of the features of the Web that made the Web successful.

Web services that use the REST architectural style are often referred to as RESTful.

An important concept in REST is the existence of resources (sources of specific information, in this case health information), each of which is referenced with a global identifier (e.g., a URI in

HTTP). In order to manipulate these resources, components of the network communicate via a standardized interface (e.g., HTTP) and exchange representations of these resources (the actual documents conveying the information).

RESTful web services are thought of by some as simpler than SOAP web services. They are resource-centric (they manipulate resources on remote systems) rather than process-centric (they do not initiate procedures on remote systems).

2.4.1.3 Privacy and Security Standards

Encryption and decryption of electronic health information is to be based on the Advanced Encryption Standard (AES) standard adopted by the U.S. government. Transport is to be over HTTP using and encrypted based on the Transport Layer Security (TLS) cryptographic protocol to provide security for communications over the Internet and the Internet Protocol Security (IPsec) protocol suite for securing communications by authenticating and encrypting each packet of a data stream. TLS is based on its perhaps more-well-known predecessor, Secure Socket Layer (SSL). Secure Hash Algorithm 1 (SHA-1), a cryptographic hash function designed by the National Security Agency (NSA), is to be used to ensure that information not be altered in transit.

The actions a system make take concerning health information records, cross-enterprise authentication, and permissible disclosures are governed by policy, not by technology.

2.4.2 Differences between the IFR and NHIN Exchange

There exist some key differences between the IFR and standards promoted by NHIN. Among them are:

1) NHIN Exchange is technically content-agnostic. However, most profiles for using NHIN Exchange make use of CCD documents, not CCR documents. NHIN Direct has not determined a preferred or standardized content format.
2) NHIN Exchange has no standard for representation of e-prescribing transactions, formulary information, structured lab results, or immunizations. NHIN Direct has not determined a preferred or standardized content format for lab results or immunizations. Other transaction types are not NHIN Direct priority use cases.
3) NHIN Exchange has an emerging standard for quality measure reporting that conforms to PQRI, as outlined by the IFR. Quality reporting is not an NHIN Direct priority use case.
4) NHIN Exchange has explored the use of CORE I standards for administrative transactions, but has no formalized standard at this time. Administrative transactions are specifically excluded from NHIN Direct priority use cases.
5) NHIN Exchange uses SOAP web services, not REST. NHIN Direct is exploring the use of REST.

3 Privacy and Security Requirements

Requirements for security and privacy cannot be addressed independent of a technical approach to addressing functional requirements for exchange. In fact, requirements associated with privacy and security might well be considered functional requirements. They are, for example, included as an explicit criteria in meaningful use.

However, it is appropriate to consider the analysis of privacy and security requirements separately from functional requirements for exchange in order to fully appreciate the impact of privacy and security requirements on exchange functionality.

3.1 NHIN Exchange Policies and Infrastructure

3.1.1 Data Use and Reciprocal Support Agreement

The Data Use and Reciprocal Support Agreement, or DURSA, is a document that governs the legal agreement among entities that exchange health information via the NHIN. The following description of the DURSA is exerted directly from the *Overview: Data Use and Reciprocal Support (DURSA) Provisions Overview* published by ONC on 20 November 2010.

- ***Multi-Party Agreement**. The DURSA must accommodate and account for a variety of Participants so that it can successfully serve as a multi-party agreement among all Participants. This multi-party agreement is critical to avoid the need for each Participant to enter into "point-to-point" agreements with each other Participant, which becomes exceedingly difficult, costly and inefficient as the number of Participants increases.*
- ***Participants in Production**. The DURSA expressly assumes that each Participant is in "production" and, as a result, already has in place trust agreements with or written policies applicable to its end users. These end user trust agreements and policies support the trust framework memorialized in the DURSA.*
- ***Privacy and Security Obligations**. To the extent that each Participant has existing privacy and security obligations under applicable law (e.g. HIPAA or other state or federal privacy and security statutes and regulations), the Participant is required to continue complying with these obligations. Participants, which are neither HIPAA covered entities, HIPAA business associates nor governmental agencies, are obligated to comply with specified HIPAA Privacy and Security Rules as a contractual standard of performance.*
- ***Requests for Data Based on Permitted Purposes**. Participant's end users may only request information through the NHIN for "Permitted Purposes," which include treatment, limited purposes related to payment, limited health care operations with respect to the patient that is the subject of the request, specific public health activities, quality reporting for "meaningful use" and disclosures based on an authorization from the individual.*
- ***Duty to Respond**. Participants that allow their respective end users to seek data through the NHIN for treatment purposes have a duty to respond to requests for data for treatment purposes. This duty to respond means that the Participant will send a standardized response to the requesting Participant, which may or may not include the actual data requested. Participants are permitted, but not required, to respond to all other (non-treatment) requests. The DURSA does not require a Participant to disclose data when such a disclosure would violate applicable law or conflict with any restrictions an individual may have placed on the data in accordance with the HIPAA Privacy Rule.*
- ***Future Use of Data Received Through the NHIN**. Once the Participant or Participant's end user receives data from a responding Participant (i.e. a copy of the responding Participant's records), the recipient may incorporate that data into its*

records and retain that information in accordance with the recipient's record retention policies and procedures. The recipient can re-use and re-disclose that data in accordance with all applicable law and the agreements between a Participant and its end users.

- ***Duties of Requesting and Responding Participants**. Each Participant has certain duties when acting as a requesting or responding Participant.*
  - *When responding to a request for data, Participants will apply their local policies to determine whether and how to respond to the request. This concept is called the "autonomy principle" because each Participant can apply its own local policies before requesting data from other Participants or releasing data to other Participants.*
  - *It is the responsibility of the responding Participant – the one disclosing the data – to make sure that it has met all legal requirements before disclosing the data, including, but not limited to, obtaining any consent or authorization that is required by law applicable to the responding Participant. This policy is essential for nationwide health information exchange given the number of different state laws, Federal statutes and local policies related to consent or authorization to exchange data for treatment purposes. To effectively enable the exchange of health information in a manner that protects the privacy, confidentiality and security of the data, the DURSA adopts the HIPAA Privacy and Security Rules as minimum requirements.*
  - *Under HIPAA, data can be exchanged for treatment purposes without obtaining a separate consent or authorization. Under some state laws and other Federal laws, however, patient consent or authorization is required to exchange data for treatment. Responding Participants who are subject to these more restrictive laws will be required to obtain those consents or authorizations that they deem necessary under their applicable laws before sending data through the NHIN. As the DURSA is written, the responsibility for obtaining this consent or authorization will not fall to the requesting Participant, usually a healthcare provider, because there is simply no way for the requesting healthcare provider to keep track of the rapidly changing laws and regulations in every state. It is unlikely that even patients will know what specific consent forms may be required for data exchange by their local Health Information Exchange (HIE). Requiring the requesting Participant to obtain a consent or authorization that complies with the responding Participant's applicable law would create an undue burden on requesting Participants. Essentially, this would require the requesting Participant to track the laws of all 50 states and federal laws beyond HIPAA and have consent or authorization forms that meet each individual state's requirements. Instead, it is more reasonable to expect each responding Participant to remain current on the legal requirements to which it is subject and take steps to comply with those laws.*
  - *When a request is based on a purpose for which authorization is required under HIPAA (e.g. for SSA benefits determination), the requesting Participant must send a copy of the authorization with the request for data. As described in the bullet above, requesting Participants are not obligated to send a copy of an authorization or consent when requesting data for treatment purposes.*

- ***Breach Notification****. Participants are required to promptly notify the NHIN Coordinating Committee and other impacted Participants of breaches which involve the unauthorized disclosure of data through the NHIN, take steps to mitigate the breach and implement corrective action plans to prevent such breaches from occurring in the future. Suspected breaches must be reported within one (1) hour of discovering information that leads the Participant to believe that a breach may have occurred. As soon as reasonably practicable, but no later than twenty-four (24) hours, Participants must notify affected Participants and the NHIN Coordinating Committee This process is not intended to address any obligations for notifying consumers of breaches, but simply establishes an obligation for Participants to notify each other when breaches occur to facilitate an appropriate response.*
- ***Mandatory Non-Binding Dispute Resolution****. Because the disputes that may arise between Participants will be relatively complex and unique, the Participants will agree to participate in a mandatory, non-binding dispute resolution process.*
- ***Allocation of Liability Risk****. With respect to liability, the DURSA memorializes the Participant's understanding that each Participant is responsible for its own acts or omissions.*
- ***Applicable Law****. The DURSA reaffirms each Participant's obligation to comply with "Applicable Law." As defined in the DURSA, "Applicable Law" is the law of the jursidiction in which the Participant operates. For non-Federal Participants, this means the law in the state(s) in which the Participant operates and any applicable Federal law. For Federal Participants, this means applicable Federal law.*

While the DURSA does not call out any specific technical or functional requirements, it is described in this document as it might be considered a model for data use agreements within the State, and thereby might dictate some policies that must be implemented or at least enabled by the underlying HIE technology.

3.1.2 NHIN Trust Framework

The NHIN trust framework comprises a messaging platform, an authorization framework, and a policy and convention for the use of patient preferences or "consent" to exchange.

The messaging platform for NHIN Exchange is based on the use of web services as established by WS-I Basic and Basic Security Profiles. They include the use of Simple Object Access Protocol (SOAP) 1.2 for web services, using Hypertext Transfer Protocol (HTTP) 1.1 for information transport with Transport Layer Security (TLS) 1.0 encryption based on Advanced Encryption Standard (AES) 128-bit symmetric encryption and X.509 Token Profile 1.0 tokens. Taken together, with other portions of the WS-I Basic and WS-I Security profiles, the messaging platform provides a secure mechanism to exchange information over the Internet based on well-supported Internet standards in common use today.

The authorization framework is based on an approach in which the initiating entity sends an "assertion" of authorization that includes the user identity, but not the identity controls (e.g., the login ID or password) of that user. The receiving or responding entity consults its local policy to establish whether to perform the requested function – provide a patient ID, respond to a query for documents or subscription for information, transfer documents, or accept submitted data. The policy may be different for each receiving or responding organization as required by its stakeholders, as long as it conforms to the provisions of the DURSA.

Importantly, it is the system or entity that is acting on behalf of the end user that takes responsibility for authentication, and asserts their identity and other credentials. The NHIN model does not support individual user authentication.

The technology of the authorization framework is based on Security Assertion Markup Language (SAML), an XML-based standard for exchanging authentication and authorization data between security domains. Among other fields, the SAML assertion includes the user's plain-text name and National Provider Identifier (NPI), the user's plain-text organization and the object identifier (OID) that unambiguously identifies it, the role of the user (e.g., Medical Doctor, Pharmacist, Administrative Healthcare Staff, Patient, etc), and the purpose for the request (e.g., Treatment, Payment, Fraud Detection, Disclosure to a Family Member, etc).

It is the combination of role and purpose-for-use that are perhaps the most important determinants in a decision to release or not release requested health information, when considered against local policy and patient preferences. Figure 1 in Section 2.2.2 *NHIN Messaging Framework* illustrates the sequence of events in determining whether to release information, which is reproduced in Figure 6 below as a reference. Other information makes up the audit trail that should capture all requests for information, whether or not they are fulfilled, and all disclosures.

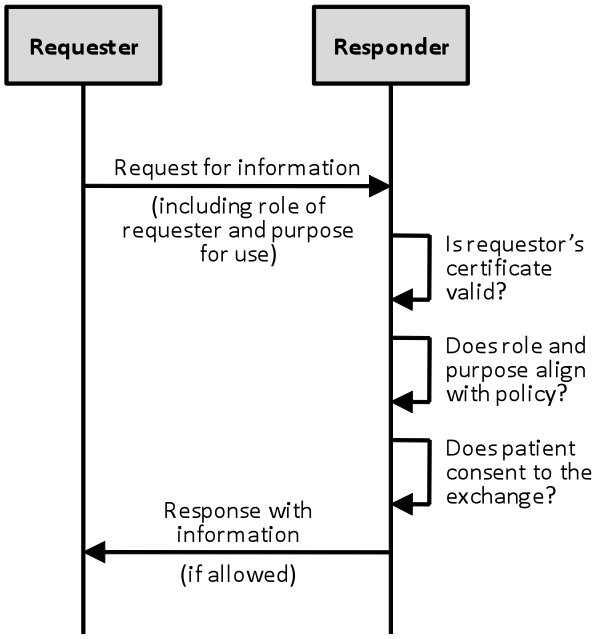

Figure 6 Illustration of the authorization and patient consent solution implemented by NHIN Exchange, repeated from Figure 1 as a reference.

The NHIN trust framework does not include a central repository for patient consent nor a mechanism for entities to exchange consent documents. Instead, it follows the principle of local autonomy. Each entity is responsible for collecting patient preferences or consent for the exchange of their health information, and implementing those preferences in line with their local policy, local law, DURSA requirements, and HIPAA.

3.2 NHIN Direct Policies and Infrastructure

At this time, NHIN Direct has concentrated on the technical services and approaches to information transport rather than policies that will govern secure exchange. Its Security and Trust Workgroup has begun to draft a trust model for NHIN Direct, but it is far from complete. However the draft model contains the following key goals:

1) NHIN Direct Implementations will support simultaneous communication across multiple secure NHIN Direct networks enabled by different trust policy frameworks in a configuration must be flexible enough to describe trust relationships at the user endpoint and organization levels. Networks with different trust and security rules may exist, each enabled by digital certificate authorities that have a single published security policy.
2) NHIN Direct Implementations must ensure that messages are delivered only to the person(s) to whom they were addressed.
3) NHIN Direct Implementations must ensure that a recipient can unambiguously identify the source of a message.
4) NHIN Direct Implementations must enable trust assertions at either the organization or user endpoint.
5) NHIN Direct Implementations must support communication with patients/individuals using pseudonymous NHIN addresses and certificates. Clinicians will trust that a given patient/individual address is associated with a given patient because the patient will personally present that address to the provider.
6) Identity assertions and trust relationships must be modeled using x.509 PKI technology but other security and trust decisions may be described in linked policy documents.
7) NHIN Direct Implementation interfaces should allow individual NHIN Direct users to think in terms of trust, rather than in PKI technical language .
8) NHIN Direct Users must be allowed to make all Trust Decisions. NHIN Direct Implementations will not automatically include any root certificate from a particular certificate authority.There will be no “default” or “central” trust authority for NHIN Direct.

3.3 State Requirements for Privacy and Security

CalPSAB has formulated a set of recommendations regarding privacy and security guidelines for exchanging health information under the State HIE Cooperative Agreement Program. The guidelines that are accepted by the Secretary will become requirements for all entities that exchange health information using resources of the State shared services.

The recommended guidelines are currently in draft form, but it is expected that many will be accepted by the CHHS Secretary. In certain cases, these guidelines go well beyond the criteria for HIE set forth in the draft rule for meaningful use and in HIPAA, making it important to consider them in planning an HIE infrastructure for California.

3.3.1 CalPSAB Recommendations and State Requirements

Notable guidelines proposed by CalPSAB include:

- *Allowable uses and disclosures of protected health information (PHI) via HIE*: Uses and disclosures of PHI for transmitting through an HIE are initially limited to clinical treatment

where a health care provider/individual relationship exists and mandated public health reporting purposes. This guideline applies to an independent health information organization, as well as to two separate health care organizations who exchange PHI without the use of a third-party organization.

- *Patient consent to transmission of PHI via HIE*: An opt-in[6] policy must be obtained to transmit PHI through an HIE for all other purposes before the information may be exchanged electronically. CalPSAB is reviewing opt-in policies, subject to State and federal law, and in consideration of the State HIE Cooperative Agreement Program with ONC, and the features of the opt-in policy may change.
- *User authentication within an entity*: An entity shall authenticate each authorized user's identity prior to providing access to PHI. An entity shall authenticate each user to the level of authorized access that complies with the entity's level of trust agreement with the external exchange entity. An entity that authenticates users attempting to access individually identifiable health information remotely from an unsecured location or device, shall require National Institute of Standards and Technology (NIST) Level 3 authentication in which the data requester must establish two factors[7] of authentication. For example, if Entity A requires two-factor authentication to allow disclosures of PHI to Entity B, Entity B will need to use two factor authenticate for its own users, at least when requesting information from Entity A.
- *Entity authentication within a "trust network"*: If an entity is participating in a trust network[8] HIE, the trust network shall manage entity authentication for those participating on the trust network, and an entity shall manage user authentication only for those entities participating on the trust network. If the user authentication process is performed across multiple systems or entities, an entity shall implement the agreed upon authentication process as specified by the requesting entity among the participants in the trust network.
- *Authorization and access control*: An entity shall use the following access control attributes to determine if a user is authorized to access requested information in a way that corresponds to, and is compliant with, the data use agreements governing such access and as it aligns with State criteria: Data Source, Entity of Requestor, Role of Requestor, Use of Data, Sensitivity of Data, and Consent Directives of the Data Subject.

---

6 As used in this context, "opt-in" refers to express permission from the patient to allow the provider to send or share PHI via the HIE.

7 Two-factor authentication requires that two separate pieces of information and processes be used to authenticate, or verify the identity of, a person or other entity. In the context of user authentication, this is often considered to be any two of "something you know, something you have, and something you are". For example, a password and security token might fulfill two-factor authentication as "something you know" and "something you have". Likewise, a password and fingerprint might be "something you know" and "something you are".

8 CalPSAB defines a "trust network" as an online environment in which parties can interact with each other securely. A trust network ensures that all members adhere to some basic principles, especially in nonrepudiation, data security, communications security, and IT security. Thus a trust network promotes trust between its members.

An entity that acts as a data requestor shall execute the authorization process at the location agreed upon in the data use agreements governing that exchange. The data requestor shall pass the authentication and authorization to the data supplier as a single message if so designated by the data use agreement.

4 Technology Strategy

The California eHealth Technical Working Group (TWG) defined a high-level architecture that outlines an approach to technology strategy that is described in the State's Operational Plan. That strategy was based on general requirements proposed by California eHealth Technical Advisory Committee (TAC) and on TWG members' own knowledge of technical requirements for HIE. Portions of that strategy are included here. However, the analysis of meaningful use criteria was the primary basis for requirements in this description, as well as the standards requirements of the NHIN and IFR, NHIN Exchange and NHIN Direct capabilities, and security and privacy guidelines.

This strategy may require some revision as the policies for security and privacy become more completely defined. In particular, the technology should enable or implement the policies that dictate privacy and patient consent, and not dictate them. Therefore, it is necessary that the key policies that address:

1) privacy and patient consent;
2) the requirements for data use and trust agreements among participants in the exchange;
3) the process for provisioning participants and monitoring their continued compliance with State policy; and
4) the needs for provider and patient authentication

occupy a very high priority in revising the technology strategy and developing an architecture for a technical solution.

What appears in this section is not an architecture for statewide shared services. Instead, it is a high-level strategy for the technology components of an architecture. The architecture itself is described in an accompanying document, *Technical Architecture for Services – Architecture*. What appears in this section is also not a design for shared services. A detailed software design is beyond the scope of the *Technical Architecture for Services*. Defining the detailed software design should instead be part of the procurement that implements those services.

4.1 Drivers in Developing a Technology Strategy

4.1.1 General Principles and Guidelines

The technology strategy for statewide shared services is informed by a set of general principles and guidelines defined by the TAC and TWG and reiterated in the Operational Plan. The following list, summarized from the Operational Plan, represents high-level requirements defined by those organizations that provide guidance for the a strategy for the HIE infrastructure in California.

- Capabilities that support providers in achieving meaningful use should occupy a high priority in the functional requirements for the technical architecture and the shared services that will be developed. However, the technical infrastructure and services

should not be bound by the meaningful use criteria, and statewide shared services should be self-sustaining and help offset the costs of building additional value-added services.

- Statewide services should support means for provider organizations of all sizes, in all locations, and serving all populations, including the vulnerable and underserved, to achieve meaningful use.
- Statewide services should complement and support, not impede, the core business and clinical processes of the intended providers and consumers of HIE services.
- Statewide services should facilitate HIE where existing resources are lacking or insufficient. Existing investments in HIE infrastructure should be leveraged, and services should not disrupt or displace existing, effective resources that are compliant with State and federal requirements.
- Near-term adoption and use of statewide services should be balanced against the requirement to have a robust long-term solution. The architecture should be flexible enough to enable a process of continuous improvement to address technology changes, new security threats, and developing technical specifications, requirements, and innovations.
- Patients and their families should be considered among the consumers and primary beneficiaries of statewide services and meaningful use of HIT, and the design should be made patient-centric whenever possible.
- The infrastructure should be secure with respect to ensuring the identities of counterparties, transmitting health information such that it cannot be disclosed to unauthorized parties or modified in transit, and in compliance with all applicable regulations and laws.
- It is not sufficient for the infrastructure to “be secure”. It must also be *perceived as secure* by stakeholders, including health care providers and the general public. The infrastructure must be paired with appropriate policies and procedures to develop the trust required to be used by stakeholders.
- Technical and security requirements of the statewide services must be consistent with and should support participating entities’ compliance with privacy and security requirements.
- Use of the statewide services developed under the State HIE Cooperative Agreement Program should be voluntary. Any stakeholder can choose to use the resources of their own enterprise, a regional HIO, or any other entity to achieve HIE. Use should also be available to any health care participant, subject to the technology requirements, operating rules, and fee requirements of the services, and restrictions or requirements of HIPAA and the HITECH provisions of ARRA.
- Design shall support interoperability with the NHIN as one emerges and with the HIE infrastructures of other states.

4.1.2 Meaningful Use Requirements

State leadership and the guidelines above have identified the support of providers in achieving meaningful use as the priority driving the functional capabilities of statewide services. The detailed discussion in Section 2.1 *Meaningful Use* outlined the requirements derived from

meaningful use, and are summarized in Table 11. Unlike Table 3 and Table 4 in Section 2.1, this table suggests some linkages between the standards-based specifications and software components.

Table 11 Summary of the requirements for technical specifications and key software components derived from meaningful use criteria.

<table>
<tr><th>Specification Requirements</th><th>Software Component Requirements</th></tr>
<tr><td>a standards-based message framework for secure and reliable exchange</td><td rowspan="3">a digital certificate authority that is supported by a standards-based interface and supporting the messaging framework and trust framework</td></tr>
<tr><td>a trust framework for authorization and consumer consent</td></tr>
<tr><td>a standards-based interface to a root certificate authority that “authenticates” an entity</td></tr>
<tr><td>a standards-based interface to a directory of all entities participating in exchange</td><td>a directory of entities participating in exchange</td></tr>
<tr><td>a standards-based interface to a directory of providers participating in exchange</td><td>a directory of providers participating in exchange</td></tr>
<tr><td>a standards-based service specification for discovering patient identities and agree on shared identities</td><td></td></tr>
<tr><td>a standards-based service specification for (1) a push exchange pattern, (2) a query and response exchange pattern, and (3) a publish and subscribe exchange pattern</td><td></td></tr>
<tr><td colspan="2">a gateway interface to the Nationwide Health Information Network</td></tr>
</table>

In the above table, the digital certificate authority supports the secure message framework and trust framework, and is supported by a standards-based specification for accessing certificates contained in it. The entity directory and provider directory are supported by standards-based interface specifications as well. There are no specific requirements for software components to support patient discovery or the information exchange patterns. In particular, there is no requirement for a statewide MPI to support patient matching.

The gateway to NHIN Exchange comprises both a software component and a set of standards-based service specifications published by ONC.

It is important to realize that all of the functional requirements listed in Table 2 must be implemented to fully support meaningful use. Unless CMS makes significant alterations in the draft rule for meaningful use, no provider can quality for incentives without demonstrating all criteria to some degree. However, it suggests that some function capabilities have a higher priority than others in demonstrating value to providers and therefore value in statewide exchange services.

1) All meaningful use criteria require authentication and network location of entities receiving information or queries for information. This suggests that a technical solution to

these requirements – a digital certificate authority and entity registry – might occupy the highest priority.

2) Secure information submission is required for more meaningful use criteria than other exchange patterns. Development of the specification for this capability might occupy a high priority.

3) Most criteria require the network locations of systems and entities rather than individual providers. Therefore, directory services that identify entities might be prioritized to proceed those that identify providers to better demonstrate value.

4) Secure information feeds supports only a single meaningful use criteria – syndromic surveillance – that might also be supported by secure information submission. A specification for it therefore might be dropped from the list of technical requirements, or at least put at the lowest of priorities.

5) An NHIN gateway is likewise only required by a single meaningful use criteria – submission of quality measures. However, access to NHIN may be required to meet the requirements of the State HIE Cooperative Agreement Program to exchange information with federal agencies and other state HIEs. Therefore, it may not be reasonable to drop it.

The meaningful use criteria specify that eligible professionals and hospitals detail specific security requirements for HIE certified EHR technology. The security requirements for EHR certification, as currently specified in the IFR, include the following provisions:

1) Health information must be encrypted when in transit through the use (at a minimum) of transport-level security mechanisms using TLS and IPSec;

2) It must be possible to verify that exchanged health information has not been altered in transit through the use of the SHA-1 secure hashing algorithm; and

3) Transactions must contain sufficient identity information about the sending party (whether that party is providing health information or requesting health information) that the receiving party can make access control decisions, and produce detailed and accurate security audit trails.

These requirements must be included in the message framework, trust framework, and certificate authority.

4.2 Proposed Technology Strategy

The overall technology strategy for statewide services to support meaningful use includes the following key components:

1) The strategy is based on a service-oriented approach to system design using the Internet.

2) The strategy includes the development of technical specifications and software components required for meaningful use as outlined in Table 11.

3) The software components may be separated into so-called “core components” that comprise the infrastructure for statewide HIE and so-called “non-core components” that provide value-added services.

4) Policy must inform the development of the messaging framework and trust framework specifications.
5) The core components implement the messaging framework and trust framework specifications.
6) The messaging and authorization framework for the statewide exchange but be consistent with the transport standards and security standards identified in the IFR.
7) The services and standards developed for NHIN Exchange should inform the development of the statewide infrastructure and be utilized or leveraged where possible.

The following discussion outlines, at a high level, the strategy for developing a system architecture for statewide exchange that includes these key strategy components. The strategy for statewide shared services adopts a system-level trust model like NHIN Exchange, where the systems organizations use take responsibility for safeguarding health information. Like NHIN Direct but unlike NHIN Exchange, the strategy provides for mechanisms to send health information to specific providers or patients on the exchange as required by meaningful use, not only the organizations in which they participate or the systems they use.

A small set of definitions help one understand the technology strategy for statewide shared services, and describe the elements of the proposed high-level system architecture and how they may interact. Certain definitions are based on ONC consensus definitions, whereas others are *ad hoc* definitions intended specifically to explain the technology strategy described here.

- *Entity*: A legal business entity that assumes responsibility for safeguarding the patient health information under its control and for managing in a secure manner the exchange of PHI. Entities may be physician practices, hospitals, clinics, pharmacies, health plans, state or federal agencies, IDNs, health systems, or HIOs. The responsibilities of Entities include ensuring that their users are reliably authenticated when they request access to PHI that is controlled by other entities, and reliably authorizing access to the PHI they control when requested by other Entities.
- *HIO*: Or health information organization, an organization that oversees and governs the exchange of health-related information among principals. HIOs may include *regional* HIOs, IPAs, or other private non-profit, private for-profit, or government Entities that oversee and govern HIE.
- *Node*: A health IT system that exists on the Internet and implements services that participate in statewide HIE in accordance with the messaging framework and authorization framework. Nodes may include EHRs, practice management (PM) systems, lab information systems (LISs), immunization registries, public health reporting and surveillance data warehouses, personal health records (PHRs) or patient-controlled health records[9] (PCHRs), health plan claims and eligibility systems, etc. Nodes are not equivalent to Entities, but are operated by them. Entities take responsibility for Nodes.
- *State Infrastructure*: Or Infrastructure, a minimal set of technical resources that enable statewide HIE, including the key standards-based specifications for the messaging

9 The patient-controlled health record is a new term that is somewhat distinguished from a PHR as a repository of clinical information under the control of a patient. Google Health and Microsoft HealthVault are two examples of PCHRs.

framework and trust framework and software components that provide entity and provider directory services that together establish a secure and reliable basis for health information exchange compliant with State policy and enabling meaningful use; managed, overseen, regulated and/or financially supported to some extent by Cal eConnect under the State HIE Cooperative Agreement Program.

- *Business Services*: A set of value-added software components and their service-oriented interfaces available to any eligible stakeholder in the California health care system, built upon and using the State infrastructure in order to enable value-added business processes; Business Services may be governed, developed, and operated by Cal eConnect, or may be developed, operated, and offered by third parties under Cal eConnect governance.

A larger set of definitions is included in the Operational Plan, but are not necessary for this discussion.

The Operational Plan also identified two sets of services – so-called "core services" and "non-core services" – that comprise the statewide architecture, as outlined by the TWG. Unfortunately, that terminology has caused some confusion among stakeholders, and a different terminology is introduced in this strategy. The State Infrastructure includes the core components identified in the Operational Plan, along with technical specifications for the messaging framework and trust framework. The Business Services[10] include the so-called non-core services.

4.2.1 Standards-based Specifications

The architecture for statewide services should be based on web services using service-oriented design principles. The specifications comprise:

- *Messaging Framework*: Specifications for the basic exchange of information over the Internet, the messaging framework is based on web services following recognized national standards. It includes specifications for the web service standard, acceptable encryption standards, and the use of digital certificates to establish secure, reliable, encrypted exchange.
- *Authorization Framework*: Specifications for how entities assert authorization for information requests, and how those assertions are carried within the Messaging Framework. The Authorization Framework must identify how the key requirements of CalPSAB authorization and access controls are addressed, including how to represent the data source, entity of requestor, role of requestor, use of data, sensitivity of data, and consent directives of the data subject are addressed. The Authorization Framework must enable both State and NHIN policies associated with patient consent.

NHIN Exchange has defined a messaging framework, authorization framework, and patient consent conventions that meet many of the needs of the Messaging Framework and Authorization Framework and requirements of the IFR, and may be used as a model. NHIN Direct is in the process of developing an alternative to the NHIN Exchange messaging

[10] In purely technical terms, the term business service is somewhat misused here. However, in this context, it should be taken to refer to a technical software implementation of a business process using service-oriented design principles.

framework that may also inform the detailed development of the Messaging Framework. Development of the Messaging Framework and Authorization Framework are informed by State policy on privacy and security. Development of those policies should take priority, as all technical solutions are based upon the specifications for the Message Framework and Authorization Framework.

In addition to the key infrastructure specifications for the Messaging Framework and Authorization Framework, the architecture should provide for at least one specification to support discovery and exchange required for meaningful use. These specifications include:

- *Patient Discovery Specification(s)*: Standards-based mechanism(s) for two entities to agree that a match exists for a patient within each entity based on the exchange of demographics allowed by State policy and local policy of the entity. The Patient Discovery mechanism(s) should conform to the Messaging Framework and Authorization Framework, and should not require the use of a statewide identifier or statewide MPI.
- *Query and Response Exchange Specification(s)*: Standards-based mechanism(s) for one entity to request health information from another and retrieve that information, conforming to requirements of the Messaging Framework and Authorization Framework, and perhaps dependent upon Patient Discovery to enable patient matching.
- *Information Submission Specification(s)*: Standards-based mechanism(s) for one entity to submit health information to another without the explicit requirement for an electronic request, conforming to the requirements of the Messaging Framework and Authorization Framework.

The infrastructure should support the development of multiple specifications for Patient Discovery, Query and Response Exchange, and Information Submission, based on the needs and available standards. For example, the IHE XCA profile calls out a mechanism for query and response that utilizes a two-step transaction based on HL7 standards, as does the HIPAA transactions that utilize a one-step transaction based on X12 standards. In some cases, specifications for Query and Response Exchange may incorporate Patient Discovery as part of the transaction, as the X12-based transaction for eligibility determination does now. It is recommended that the State develop and adopt a small set of specifications for Patient Discovery, Query and Response Exchange, and Information Submission that it encourages, or perhaps requires, all participating organizations to support. These specifications should be compliant with requirements of the IFR. However, it is also recommended that the State allow additional standards-based discovery and exchange patterns between organizations, as long as they conform to State policies, in order to foster innovation and enable new Business Services.

NHIN Exchange has defined web service specifications for patient discovery and query/response exchange patterns that may meet the needs of statewide exchange for Patient Discovery and Query and Response Exchange. Both NHIN Exchange and NHIN Direct are developing web service specifications for a push pattern that could be used for Information Submission.

The above list may be extended to include a specification for Information Feeds. An examination of the requirements for meaningful use identified information feeds as a need. However, information feeds support only a single meaningful use criterion – public health surveillance – that could also be supported, perhaps, through Information Submission. Therefore, the development of a specification or specifications for Information Feeds should be

considered a lower priority. NHIN Exchange has defined web service specifications for information feeds.

In addition, the core services are accessed through standards-based service-oriented interfaces described by specifications. The details of those specifications are included in Section 4.2.2 *State Infrastructure* below.

Cal eConnect should take responsibility for developing the specifications for the Messaging Framework, Authorization Framework, Patient Discovery, Query and Response Exchange, and Information Submission through an open and transparent process that includes stakeholders throughout the State. The development of these specifications *must* be preceded by definition of the policies that define privacy and security, and the role and process for patient consent. There exist several models for standards development, including perhaps the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C), and IHE. An analysis of the commonalities among these three recommends a set of best practices that include:

1) An open, inclusive process including input from a board industry cross-section, not only for public comment, but likewise for the drafting of new specifications.
2) A controlled, transparent mechanism for prioritizing development of new specifications and advancing them through the development process.
3) A managed and documented model for the maturity of a developing specification that defines the roles of all participants at each stage of development.
4) A process to subject specifications to implementation testing to assess whether a specifi-cation is complete and can be implemented.

If the specifications of NHIN Exchange and developing specifications of NHIN Direct are appropriately leveraged, it should be possible to complete this action through a minimal technical staff working with volunteers from the stakeholder community in working groups and in a short period of time.

4.2.2 State Infrastructure

The architecture for statewide services requires a small set of software components, with standards-based service-oriented interfaces to them, in order to support providers in achieving meaningful use. The State Infrastructure is intended to create a foundation for organizations and participants to exchange health information across their organizational boundaries, such that two Entities that have not necessarily exchanged information previously can find each other, positively identify each other in a trusted manner, determine where and how to effectively exchange health information, exchange information in a secure manner that supports both authorization decisions and the appropriate logging of transactions, and reconcile the identity of the individual patient to whom the information pertains.

The Infrastructure comprises the technical specifications for the Messaging Framework and Authorization Framework, together with software components that provide for entity directory services, provider directory services, and entity authentication. The software components of the Infrastructure must conform to the Messaging Framework and Trust Framework, and in fact implement and enable components of it.

The Operational Plan called for a set of so-called core services that in this strategy are part of the Infrastructure, comprising an entity registry service and a provider directory service. A more complete analysis of the functional and technical requirements of the meaningful use criteria

and national standards suggest that the capabilities of these services be restructured and renamed.

- *Entity Registry*: The Entity Registry provides a trusted registry of Entities engaged in statewide exchange and the Nodes or systems for which they are responsible. The Registry serves to ensure parties engaged in exchange of the validity and authenticity of exchange partners. It also provides the primary control point for the State to enforce policies associated with health information exchange. Only Entities and Nodes with valid entries in the Entity Registry can exchange information using statewide services.

  Entries in the Entity Registry are bindings of Nodes to public encryption keys used to establish a trusted, secure, and encrypted connection for exchange. These bindings are typically represented as *digital certificates* that are signed by a trusted, centralized *certificate authority*.

  A cardinal element of the Registry Service is that its entries are trusted as legitimate and accurate by all stakeholders participating in statewide exchange. This trust requires a rigorous process for provisioning Entities and Nodes and a timely process for modifying entries in the registry (including revoking entries) as information about the Entities or Nodes changes. It therefore is a high priority that the State develop policies for how Entities are provisioned, which might include:

  a) whether the Entity has signed a State-sanctioned data use agreement, should one be required;

  b) whether the Node(s)[11] have passed technical testing to conform to specifications for the Core Services;

  c) whether the Node(s) have passed technical testing to validate that they properly implement the required discovery and exchange patterns, if called for by policy; and/or

  d) conformance to other State policies or technical requirements.

  The Entity Registry comprises a data store of Entity and Node names, descriptors that allow the Registry to be searched, and digital certificates, accessed through a standards-based web service. The Entity Registry Service is similar in concept to the NHIN Exchange Certificate Authority. The Entity Registry provides essentially the same services as the entity registry service outlined in the Operational Plan

- *Service Registry*: The Service Registry provides information about how and where to direct information intended for specific individuals or systems, such a providers or their specific EHRs, and how to formulate the transactions such that they can be correctly processed when received.

  The Service Registry provides the same services as the provider directory service identified in the Operational Plan, with a somewhat different architectural structure than that suggested there. The Service Registry provides directory services for individual providers, physician practices, hospitals, hospital departments, laboratories, pharmacies, personal health records, immunization registries, payers and any other entities to whom

[11] A single Entity may operate one or more Nodes.

health information could be legitimately sent or from whom health information could be requested.

The Service Registry should be a federated service that allows Entities to publish the address(es) at which their providers accept specific types of health information and the communication protocol(s) they support for these transactions. Through the Service Registry, this information is available to any Entity who wishes exchange information.

Entries in the Service Registry provide mappings from an individual or system within an Entity for a particular transaction to a web services address and protocol.

Entity + individual + transaction type *maps to* **web service address + protocol**

The combination of web service and protocol define the "service" used for the transaction, and therefore the name for the Registry. The Service Registry comprises a federated data store[12] of providers, other individuals, systems, descriptors that allow the Service Registry to be searched, mappings to Entities, transaction types, web service addresses, and protocols, accessed through a standards-based web service. It may also include digital certificates for entries, if State policy requires individuals to sign messages that return health information rather than implement a system-level trust model. As stated before, the Service Registry is federated, in that it may return information actually stored and maintained by Entities.

- *NHIN Gateway*: The NHIN Gateway provides a secure mechanism to bridge between the State Infrastructure and statewide exchange and the Nationwide Health Information Network. It provides the primary means for enabling exchange with federal agencies, and a means for exchanging with other statewide exchanges using a mechanism conforming to nationwide standards that is promoted by ONC.

  Development of an NHIN Gateway as part of the State Infrastructure does not preclude individual Entities in the State from also developing NHIN gateways and participating in NHIN directly. However, it reduces the burden of individual organizations in conforming to all of the technical requirements of the NHIN. It also provides hierarchical organization to the NHIN which will be necessary as the NHIN grows.

  Cal eConnect should take responsibility for the State being an NHIN exchange partner by participating in the NHIN on-boarding process, and procure an NHIN Gateway. The open-source CONNECT project may be leveraged for this purpose, or an existing HIO within the State already having NHIN capabilities may offer this service.

The Operational Plan also identifies a provider identity service as a potential core service to be included in the Infrastructure. However, an analysis of meaningful use and of the security and privacy requirements of HIPAA and the State have not identified this component as a requirement. It may be added to the State Infrastructure at a later time if required by State policy or to establish the perception of trust.

Cal eConnect should take responsibility for developing the service interface specifications for the Entity Registry and Service Registry, and procuring or building components of it. A more complete strategy for procurement will be outlined in the Architecture that accompanies this

[12] The details of the federation of the Service Registry is beyond the scope of this technology strategy document, and will be described in the architecture for State Infrastructure.

document. The specifications should be developed through an open and transparent process similar to that used for the other specifications outlined in Section 4.2.1 *Standards-based Specifications* above. The software components themselves can be developed by staff hired by Cal eConnect or, perhaps more appropriately, procured from vendors, software developers, or systems integrators as appropriate.

If the specifications of NHIN Exchange and developing specifications of NHIN Direct are appropriately leveraged, it should be possible to complete the development of the service interface specifications through a minimal technical staff working with volunteers from the stakeholder community in working groups and in a short period of time. Software components implementing the Entity Registry and Service Registry should be based on widely-accepted standards-based technologies. Therefore, the RFP process for procuring the components should be relatively simple to draft, respond-to, and assess.

Figure 7 illustrates the interaction between the Entity Registry, the Service Registry, an Entity, and a provider within another Entity in exchanging information through an Information Submission exchange pattern.

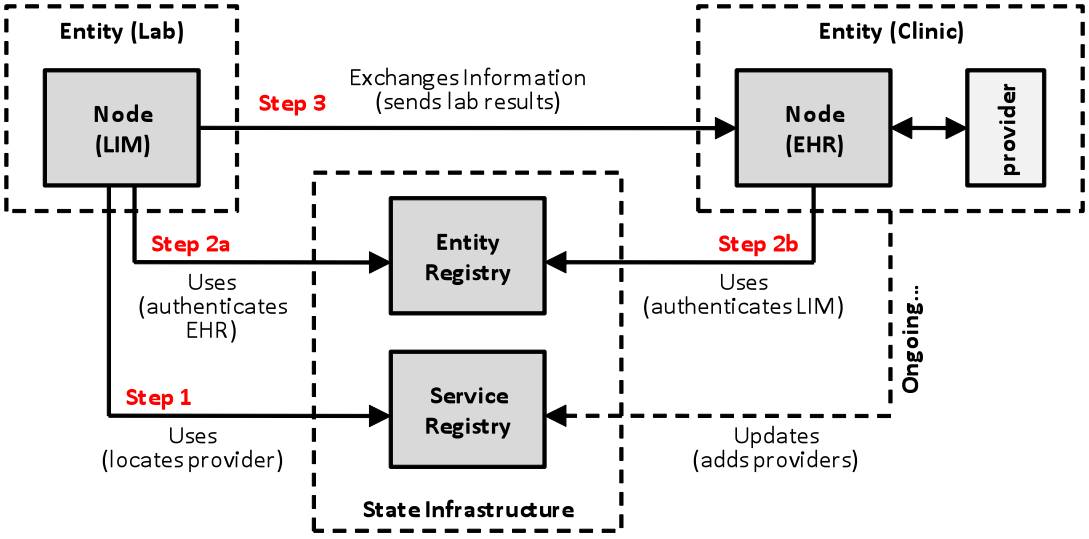

Figure 7 High-level view of the State Infrastructure components and key stakeholders, and their interrelationships within the technology strategy.

As an example, consider the meaningful use criteria in which a lab needs to send structured lab results to be incorporated into a provider's EHR. The lab identifies the intended recipient provider based on the lab order, and looks up the provider's service for receiving lab results – most likely an interface to an EHR within the provider's clinic, hospital, or HIO – in the Service Registry. The Service Registry returns a Node identifier, web service address, and protocol, which may conform to the Information Submission Specification implemented by the provider's EHR using a standards-based web service. The lab then looks up the Node for the EHR in the Entity Registry, obtaining a digital certificate that is used to create a secure and encrypted connection to the Node (and only to that Node), over which the lab result can be transferred. The clinic likewise looks up the Node for the LIM in the Entity Registry, validating the origin of the information and completing the secure, encrypted connection. Finally, the information is transfered using the web service address and protocol from the Service Registry.

4.2.3 Traceability of Infrastructure to Meaningful Use Requirements

Table 12 below summarizes the traceability between the standards-based specifications and core software components and the requirements of meaningful use.

Table 12 Traceability illustrating how the infrastructure components fulfill the technical requirements of the meaningful use criteria that require or benefit from HIE.

Meaningful Use Requirement	Infrastructure Component
a standards-based message framework for secure and reliable exchange	*Messaging Framework*
a trust framework for authorization and consumer consent	*Trust Framework*
a standards-based interface to a root certificate authority that "authenticates" an entity or individual	*Entity Registry*
a digital certificate authority that is supported by a standards-based interface and supporting the messaging framework and trust framework	
a standards-based interface to a directory of all entities participating in exchange	*Entity Registry* and *Service Registry*
a directory of entities participating in exchange	
a standards-based interface to a directory of providers participating in exchange	*Service Registry*
a directory of providers participating in exchange	
a standards-based service specification for discovering patient identities and agree on shared identities	*Patient Discovery Specification*
a standards-based service specification for (1) a push exchange pattern, (2) a query and response exchange pattern, and (3) a publish and subscribe exchange pattern	*Query and Response Exchange* and *Information Submission Specifications*
a gateway interface to the Nationwide Health Information Network	*NHIN Gateway*

4.2.4 Business Services

In addition to the State Infrastructure described above, providers may be supported in achieving meaningful use through additional value-added Business Services. These additional Services may be provided through a number of potential business models.

1) Cal eConnect might procure development and integration services from a vendor, software developer, or systems integrator, and have the service delivered to Cal eConnect and operated by as a continuing source of revenue.
2) Cal eConnect might procure the service to be developed and operated by a vendor or systems integrator, and simply govern its operation, perhaps for a small transaction or access fee.

3) Cal eConnect might support a local stakeholder, such as an HIO, through a grant to expand an existing service to extend it to the entire State.

4) A vendor with an existing solution may approach Cal eConnect or be solicited by Cal eConnect with a business model to offer the service in collaboration with the State.

These services provide specific business functions that are not otherwise available to eligible providers. These services would be layered on top of the State Infrastructure and developed and offered on an as-needed basis over time.

Table 5 in Section 2.1.2 *Technical Requirements Analysis* identified a number of potential Business Services that would support meaningful use. One specific Business Service is planned at this time:

- *Lab Results Clearinghouse*: A value-added service that aids labs in routing lab results to the appropriate ordering providers and public health agencies. This service would ostensibly replace the numerous point-to-point connections among laboratories, EHRs, and public health databases with a single routing hub connected to participating entities. It would utilize the Service Registry to identify the appropriate provider EHRs and/or public health agency data warehouses for delivery, and might also include translation or transformation services that aid the lab in providing lab results in a format and using a protocol supported by each.

Figure 8 provides a high-level view of how the Lab Results Clearinghouse might be used by a lab to deliver structured lab results, and how the Service interacts with the State Infrastructure to accomplish this task.

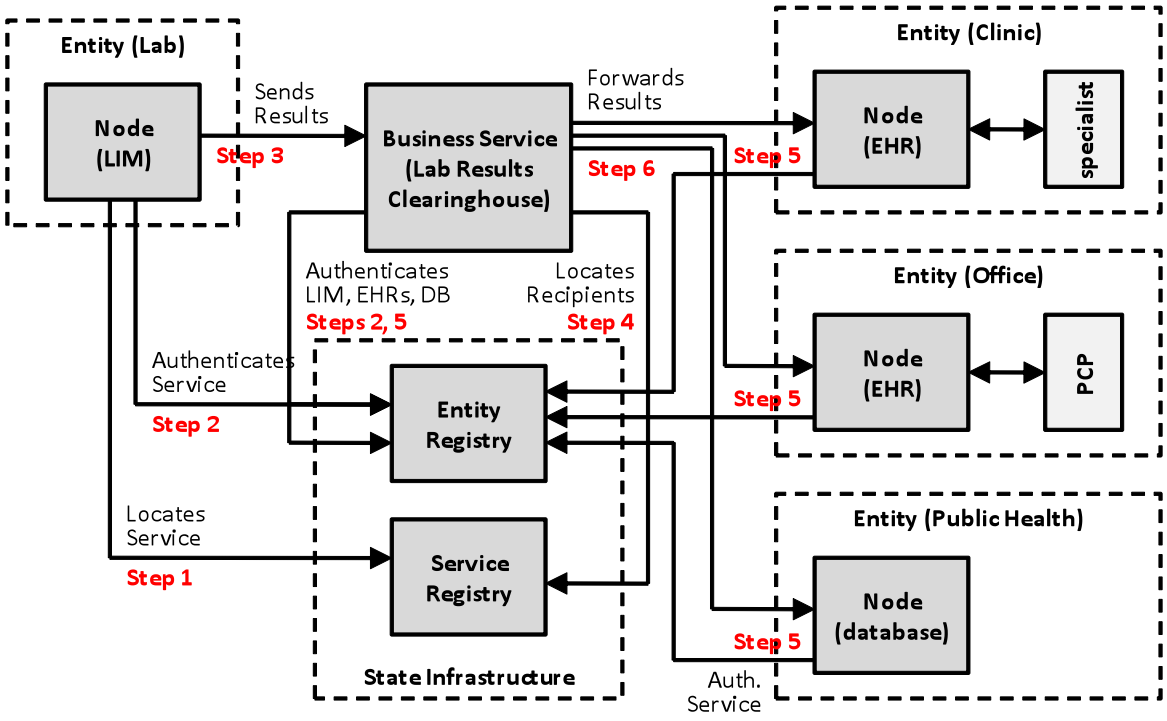

Figure 8 High-level view of the Lab Results Clearinghouse and its interaction with State Infrastructure, labs, and recipients of lab results.

In this example, the lab locates the Clearinghouse Business Service in the Service Registry, which returns an address and protocol for a Node – a web service application server that is part of an Entity providing the service. The LIM and Business Service both use the Entity registry to look up each other's digital certificates in order to establish a secure, encrypted connection over which the LIM sends the structured lab results.

The Clearinghouse Business Service responds by performing the heavy lifting of distributing the results to their intended recipients. It looks up all potential recipients in the Service Registry – a list that might include the specialist ordering the lab test, the primary care physician that referred the patient to the specialist, and a public health surveillance system if the lab test is a reportable condition or part of a syndromic surveillance protocol. In turn, it establishes secure, encrypted connections with each EHR or database using digital certificates in the Entity Registry, and forward the lab results, optionally transforming or translating the results to conform to the protocol and terminology requirements of the recipient.

The above solution is only one option for the proposed Business Service. The final solution might look different. However, the key characteristics of the Business Service are:

1) the Business Service is a Node on the statewide exchange, like any other Node;
2) an Entity Node uses the State Infrastructure to contact the Business Service;
3) the Business Service may do processing on behalf of the lab, which is a part of the value offered by the Service; and
4) the Business Service likewise uses the State Infrastructure to locate and forward any information to the intended recipients.